IEC 62304: Medical Device Software - Life Cycle Processes

Software Safety Classification, Risk Management Integration (ISO 14971), and Verification Rules

CRITICAL GOVERNANCE PRINCIPLE (IEC 62304 (CLAUSES 4, 5, 7 & 8)): Software controls are classified as programmable risk mitigation elements. Under international functional safety law, software cannot be certified in isolation from physical hardware interlocks. Independent verification (Level I1/I2/I3) and multidisciplinary sign-off are mandatory requirements prior to operational release.

1. Safety Classification & Risk Management

IEC 62304 defines life cycle requirements for software in medical and health-critical cyber-physical systems, harmonized with ISO 14971 risk management.

Clause 4.3: Software Safety Classification

Software is classified based on the severity of harm prior to software risk control measures:

- Class A: No injury or damage to health is possible.
- Class B: Non-serious injury is possible.
- Class C: Death or serious injury is possible.

Clause 7: Software Risk Management Process

Clause 7.1 requires identification of software items that can contribute to a hazardous situation. Critical principle: Software risk controls cannot be credited with reducing risk unless verified by an independent party.

- Evaluating Secondary Hazards: Risk control measures implemented in software must be analyzed to ensure they do not introduce new hazards.
- Verification of Effectiveness: Every software risk control must have documented, verified test evidence.