Sketching Verification

This is a sketch of a verification strategy for a safety goal.

Object: <new product name>
Quality goal: safety, general
Perspective: users and operators
Immediate supporting goals: dependability

Development tasks

Achievement and initial verification of all supporting quality goals (> 24)

Inspection scope: completeness and accuracy of Hazard Analysis and Failure Modes & Effects Analysis and their resulting safety hazards along with effectiveness of proposed safety mechanisms i.e. mitigations

Predesigned test scope: all safety mechanisms and built-in tests. Product misuse and unusual use tests

Analysis scope: modified condition/decision coverage (MC/DC) for safety mechanisms and access conditions

Predesigned test acceptance criteria: failure-free execution of all tests with complete MC/DC coverage as assessed by a coverage analyzer

Preproduction tasks

Limited-release testing with monitoring for safety-related incidents. Incidents include problems with any quality attribute supporting safety.

Limited-release test acceptance criteria: At least 120 accident-free days, if each previous loss is less than $1,000 USD, otherwise at least 240 accident-free days.

Production tasks

Aggressive monitoring of accidents reported to the support center, with rapid analysis of accidents, and rapid correction, if appropriate. Perform root cause analysis on each accident and look for patterns.

Tracking: accident-free days, mean-time between accidents, mean-loss per accident, and greatest loss

[This sample contains minimal information. You can add or reference as much detail as you think necessary.]