Fundamental Principles and Benefits of Explicitly-Designed Medical Device Safety Architecture

Brian R Larson

Scott Stubbs

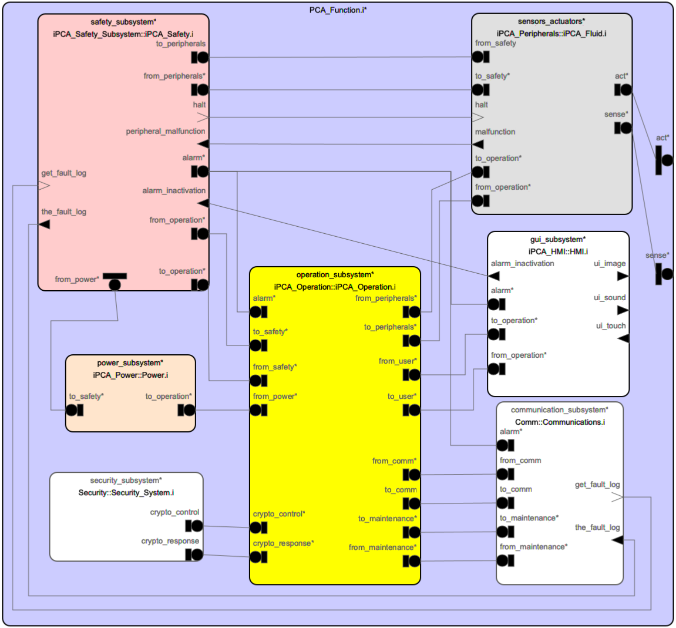
April 17, 2024

Medical device *safety* is defined as freedom from unacceptable risk.

All foreseeable risks have been mitigated to the extent practicable and the overall residual risk is acceptable.

The term *architecture* refers to the physical and logical organization of a device, especially decomposition of the device into constituent parts and the relationships and communication among those parts.

Achitecture



A *medical device safety architecture* notionally partitions the operational device design into operational and safety subsystems in which the safety subsystem monitors the operational subsystem to

- *detect* faults or failures or use errors (e.g., incorrect user input or action),
- acts to *mitigate* hazardous situations due to such events,
- *notifies* a user of such events, and
- *records* the occurrence of the fault/failure for future analysis.

By *explicit*, we mean intentionally designed and clearly documented in device development.

FDA Says:

Although these concepts are understood and followed by some device manufacturers, the authors' experience in interacting with product design teams, serving on medical device standards committees, and reviewing medical device regulatory submissions indicates overall device safety could be improved throughout the community if more manufacturers and reviewers understand these concepts and how to apply them.

Detection is the continuous function of monitoring the device for undesired states.

A detect action typically involves:

1. realizing a sensing capability to observe the physical or system phenomenon associated with the cause(s), and
2. evaluating sensor data to determine when the state of the phenomenon corresponds to the cause(s) to be mitigated.

The safety subsystem monitors device operation to ensure those components are functioning as designed.

Notification is the function of raising an alarm or warning.

The safety subsystem should be designed to include general-purpose infrastructure for alarm notification.

Mitigation is the function of reducing the risk of an undesired device state to an acceptable level of risk state.

The safety subsystem will control the actuations necessary to move the device to a known safe state.

Recording is the function of saving enough state information to reconstruct events leading to an undesired state.

Use errors prevented by the operational subsystem can be recorded in the same software log that records all device actions.

Device malfunction must be recorded in a dedicated hardware log because the malfunction may prevent execution of threads by the processor.

Device function then may be partitioned as much as possible between normal operation and safety functions that override hazardous situations in normal or abnormal operation.

1. Identify device function and known and foreseeable use hazardous situations.
2. For each hazardous situation, identify the cause(s) and acceptable risk.
3. Design, implement, and verify risk control measures.

Realization of a safety architecture includes the following activities in support of the activities in clause 6 of 14971:

1. partition device system safety decisions into safety and operational subsystems, and
2. verify safety architecture is complete and consistent with respect to safety decisions.

FDA Sponsored MBSE Example Design Artifacts . . .

. . . because designs using best practices were proprietary.

Requirements following FAA's Requirement Engineering Management Handbook: stakeholders → goals → use case maps → requirements → functional architecture.

Architecture: partitioning, interfaces, formal behavior specification, state machine implementation, deductive correctness proofs.

Assurance Case: persuasive argument of safety and effectiveness, links requirements, architecture, implementation, verification artifacts.

Frontier

PADL, Safety Architecture, Product-Line Engineering

Questions?

https://pubmed.ncbi.nlm.nih.gov/28934584/

https://array.aami.org/doi/epdf/10.2345/0899-8205-51.5.380