

F.5.7 SOFTWARE SAFETY

Objective

The design of the safety software components are developed in a manner that ensures the software modules will perform their intended safety function in a consistent manner during design bases conditions.

Criteria:

1. Software systems are analyzed at the component level to ensure adequate safeguards are implemented to eliminate or mitigate the potential occurrence of a software defect that could cause a system failure.
2. Safety software is designed with simplicity and isolation of safety functions.
3. Where appropriate fault tolerance and self-diagnostics are implemented in the safety software design.

Approach:

- Review hazard analysis documents to ensure that software component and interface failures are included. This analysis may be part of a software or system level failure modes and effects analysis, fault-tree analysis, event-tree analysis or other similar analysis techniques.
- Review how the identified hazards are resolved. Various methods are used for hazards resolutions, such as eliminations, reduction of exposure, and controlling or minimizing the effects of a hazard.
- Review that the hazard analysis is periodically reassessed throughout the software life-cycle and the changes incorporated as appropriate.
- For Level A safety software, and optionally for Level B safety software, sample safety software modules for proof of design complexity evaluation and isolation of safety functions from nonsafety functions.
- For Level A safety software, and optionally for Level B where safety software modules defects could impact the safe operation of the system, evaluate the software design for the implementation of fault tolerant and/or self-diagnostics techniques.