

F.5.6 SOFTWARE DESIGN AND IMPLEMENTATION

Objective:

The safety software design depicting the logical structure, information flow, logical processing steps, data structures and interfaces are defined and documented. The design is properly implemented in the safety software.

Criteria:

1. The design, including interfaces and data structures, is correct, consistent, clearly presented, and feasible.
2. The design is completely and appropriately implemented in the safety software.
3. The design requirements are traceable throughout the software life-cycle.

Approach:

Review the appropriate documents, including design documents, review records, and source code listings. The design may be documented in a standalone document or embedded in other documents.

- The software design description should contain the following information.
 - A description of the major safety components of the software design as they relate to the software requirements, and any interactions with nonsafety components.
 - A technical description of the software with respect to control flow, control logic, mathematical model, data structure and integrity, and interface.
 - A description of inputs and outputs including allowable or prescribed ranges for inputs and outputs.
 - A description of error handling strategies and the use of interrupt protocols.
 - The design described in a manner suitable for translating into computer codes.
- Evidence of reviews of the design and code for the appropriate grading exists. This may overlap with the software V&V work activity.
- Evidence of developer testing including any independent testing for the appropriate grading exists.