IEC 61508: E/E/PE Design and Development

Techniques and measures required for safety equipment

A. Hardware

The following is a very high-level, brief checklist from IEC 61508 part 2, Annex B. IEC 61508 is a very complex standard, and reference should be made to the standard for the necessary detail.

The degree to which each technique or measure has to be implemented depends on the SIL level required for the equipment. Not all techniques and measures are required for all SILs. Definitions of terms are given in IEC 61508 part 7.

During design and implementation

1. Robust project management and documentation (throughout)
2. Structured specification, design
3. Observance of guidelines and standards
4. Functional testing, analysis
5. Operation and maintenance instructions, user- and maintenance-friendly
6. Interference testing
7. Fault insertion testing

During operation

1. Program sequence monitoring and on-line monitoring or testing
2. Power supply monitoring and protection
3. Spatial separation
4. Ambient temperature protection
3. Modification protection

IEC 61508: E/E/PE Design and Development

Techniques and measures required for safety equipment

B. Software

The following is a very high-level, brief checklist from IEC 61508 part 3, Annex A. IEC 61508 is a very complex standard, and reference should be made to the standard for the necessary detail.

The degree to which each technique or measure has to be implemented depends on the SIL level required for the equipment. Not all techniques and measures are required for all SILs. All techniques and measures are important: some of the most important elements are in **bold**. Definitions of terms are given in IEC 61508 part 7.

1. **Functional safety assessment**: checklists, truth tables, failure analysis, CCF analysis, reliability block diagrams
2. **Software requirements specification** – formal or semi-formal methods, traceability, software tools
3. Fault detection, error detecting codes
4. Diverse monitoring techniques
5. Recovery mechanisms or graceful degradation
6. Modular design
7. Trusted/verified software elements
8. **Forwards/backwards traceability at all stages**
9. Structured or semi-formal or formal methods, auto-code generation
10. Software tools
11. Guaranteed maximum cycle time, time-triggered architecture, maximum response time
12. Static resource allocation, synchronisation
13. Language selection, suitable tools
14. Defensive programming, modular approach, coding standards, structured programming
15. **Testing**: dynamic, functional, black box, performance, model-based, interface, probabilistic
16. Process simulation, modelling
17. **Modification/change control**: impact analysis, re-verification, revalidation, regression testing, configuration management, data recording and analysis
17. **Verification**: Formal proof, static analysis, dynamic analysis, numerical analysis

IEC 61508: E/E/PE Design and Development

Techniques and measures required for safety equipment

C. ASICs and FPGAs

The following is a very high-level, brief checklist from IEC 61508 part 2, Annex F. IEC 61508 is a very complex standard, and reference should be made to the standard for the necessary detail. Annex F contains separate tables for ASICs and FPGAs; the following summarises and merges these tables.

The degree to which each technique or measure has to be implemented depends on the SIL level required for the equipment. Not all techniques and measures are required for all SILs. Definitions of terms are given in IEC 61508 part 7.

1. Structured description, VHDL design description and simulation, Boolean design description
2. Proven in use VHDL simulators and design environment
3. Functional testing on module and top levels, and embedded in system environment
4. Avoid asynchronous constructs, synchronised primary inputs
5. Design for testability; modularisation
6. Code guidelines adherence, code checker, defensive programming
7. Documentation of simulation results
8. Code inspection, walk-through
9. Validation of soft-cores
10. Internal consistency checks
11. Simulation of gate netlist to check timing constraints; static timing analysis of propagation delay
12. Verification of gate netlist
13. Check ASIC vendor requirements and constraints
14. Documentation of synthesis constraints, results and tools; use of proven in use tools and target libraries
15. Script based procedures
16. Test insertion and test pattern generation
17. Placement, routing, layout generation
18. Proven in use chip technology and manufacturing, QA, QC
19. Test coverage of manufacturing test; final verification and validation
20. Burn-in test