NDIA
51st Annual Fuze Conference
May 23-24, 2007

The DoD Fuze Engineering Standardization Working Group's (FESWG) Technical Manual for the use of Logic Devices in the Implementation of Safety Features

John D. Hughes
Naval Air Warfare Center, China Lake CA
Safe-Arm Development Branch, Code 478300D
COM (760) 939-7405
DSN 437-7405, FAX (760) 939-6562
john.d.hughes@navy.mil

Scope

- Increased use of logic devices in safety features has highlighted the need to address safety requirements in more detail.

- Document is intended to clarify the requirements of the current standards (MIL-STD-1316, MIL-STD-1911, MIL-STD-1901 and STANAG-4187, STANAG-4497, STANAG-4368) as applied to Safety Features implemented with logic devices.

- Logic Devices include programmable logic devices (PLDs), complex programmable logic devices (CPLDs), field programmable gate arrays (FPGAs), application specific integrated circuits (ASICs), microcontrollers, discrete logic, etc.

Definitions

- **Common Cause Failures. Multiple component failures that result from or are caused by a single failure or an adverse environment.**

- **Safety Feature. An element or combination of elements designed to prevent unintended arming and/or functioning. All the components from the environmental sensing, environment verification, and safety interlock are included in the safety feature.**

Disclaimer

- While some logic devices may be viewed as better suited for safety applications, it is important to note:
  - All logic devices can be implemented in an unsafe manner.
  - There are safety issues associated with the use of any type of logic device in safety critical applications.
  - Individual technologies may require additional measures not specifically addressed here.

- This presentation does not contain all the information found within the FESWG Tech Manual

Requirements

1. **Each Safety Feature (SF) implemented with logic shall use the least complex logic device that can practically perform the required functionality.**
   - **Minimizes the subversion of SF(s) due to unintentional and/or unrecognized modes of operation, including failure modes.**
   - **KISS method.**
   - **Complex devices require more analysis, documentation, testing and more scrutiny by the safety authority.**

2. All logic devices used in the implementation of a safety feature shall be non-reconfigurable
   - Stability of SF is required.
   - Changes to the SF can comprise safety.
   - Programmable devices may be considered non-reconfigurable if the configuration of the internal logic can not be changed intentionally or inadvertently after programming during manufacturing.
   - Applies to associated memory (no volatile or erasable memory allowed!).

Requirements

3. Where all SFs are implemented with logic devices, at least two SFs shall be implemented with dissimilar logic devices.
   - Minimizes the potential for common cause failures.
   - Where practical, at least one SF shall be implemented with discrete component(s).
   - Dissimilar logic refers to distinct methods and/or materials used to develop a particular device that result in devices with minimal common cause failures. Some examples include:
     - Full Custom ASIC
     - Discrete components
     - M2M FPGA
     - OnO FPGA
     - Microcontroller

Requirements

4. SF logic shall be implemented in accordance with the device manufacturer's latest specifications and notes.
   – Safety critical details could be buried within data sheets and/or footnotes.
   – Conflicts between manufacturer's specifications and other requirements shall be reviewed and approved by the safety authority.
   – All programming functionality, testing functionality, used pins, and any other non-operational functionality shall be appropriately disabled and terminated.

Requirements

5. **Logic devices shall not exhibit unsafe operation during and after exposure to power transfers, transitions, and/or transients.**
   - Credible power environments (brown out, surge, spikes, etc) should not cause the loss of a safety feature.
   - Logic device power supplies need to be robust.

6. **Timing functions within logic shall not be susceptible to single point or common cause failures resulting in early arming.**
   - Requires independent timing with dissimilar technology.

Requirements

7. **Logic implementation shall replicate the documented design.**
   – Ensures the intended design is actually implemented.
   – No optimizations or changes to an approved design.
   – Know your design tools.

8. **Where all SFs are implemented with logic devices, the SF logic shall be physically and functionally partitioned from each other.**
   – Minimizes the potential for inadvertent subversion such as sneak paths or Single Event Upsets.

Requirements

9. All logic and/or functionality available within a device shall be disclosed, documented, and assessed in safety analyses and evaluations.
   – Undocumented functions within a SF can compromise the safety of the design and is unacceptable.
10. SF documentation shall include the complete logic flow with all inputs and output defined, along with timing and interdependence of events.
   – Assists with design understanding and verification.

Requirements

11. Manufacturing documentation and processes shall ensure that logic devices within an approved design are produced with an identical configuration.
    - Assures logic devices are reproduced consistently throughout production.

12. Development tools shall be documented and controlled via configuration management procedures.
    - Assures logic devices configuration matches the intended design.
    - Know your tools and document them.

Requirements

13. Reset functions shall not be susceptible to single point or common cause failures that result in unsafe states.
    – Redundant resets with different implementations.
    – Logic device reset circuitry must be extremely robust.

Requirements

14. Power for SF logic should be partitioned from other power such as communication or platform power.
    – Minimizes subversion of a safety feature

15. Power for SF logic should be applied as late in the launch sequence or operational deployment as practical.
    – ESAD without power = SAFE

- A copy of the technical manual may be obtained via mail from the following:

Chairman

DOD Fuze Engineering Standardization Working Group

U.S. Army Armament Research, Development and Engineering Center

ATTN: AMSRD-AAR-AEP-F

Picatinny Arsenal, NJ 07806-5000

Questions???

Comments??