55th Annual NDIA Fuze Conference
May 25th, 2011

Evolving Requirements for the Use of Logic Devices in the Implementation of Safety Features
or
An Update to the DoD Fuze Engineering Standardization Working Group's (FESWG) Technical Manual for the use of Logic Devices in Safety Features

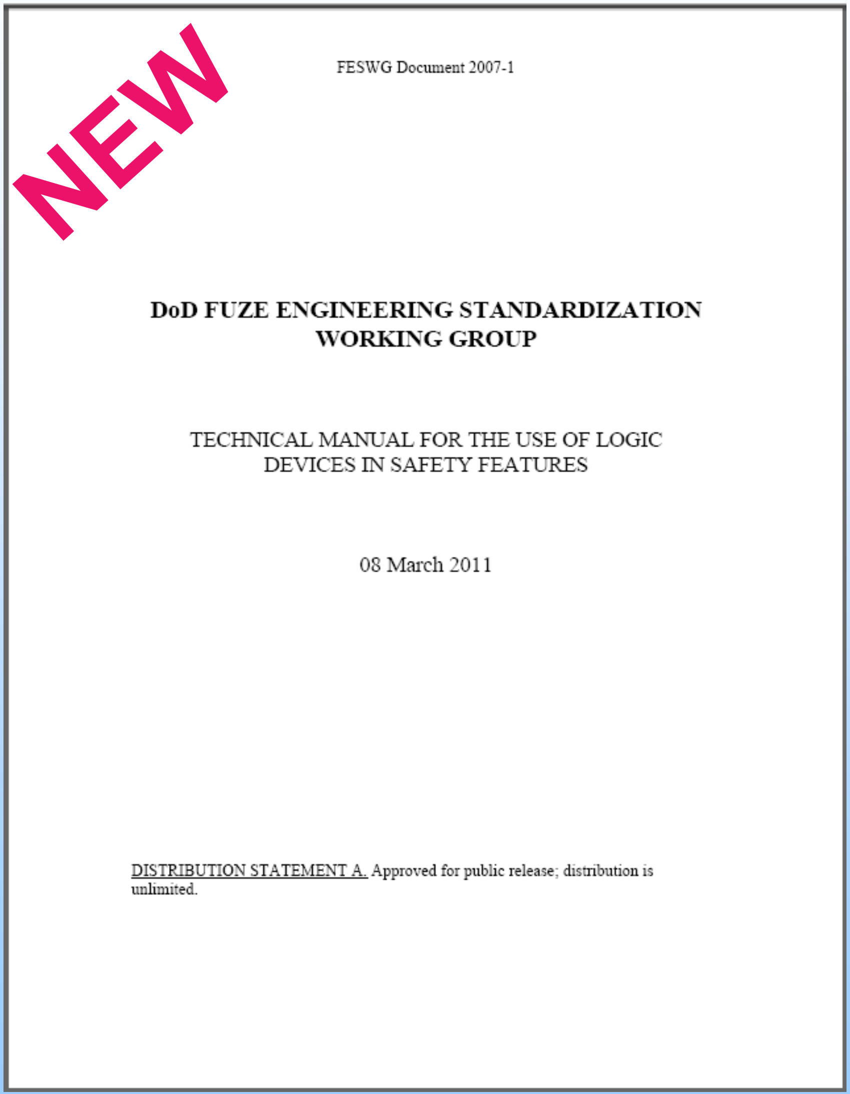
John D. Hughes
Naval Air Warfare Center, China Lake CA, 93555
Safe-Arm Development Branch, Code 478300D
john.d.hughes@navy.mil

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited

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
- Presenter does not speak for the Safety Boards. Consult your Safety Authority for current requirements.

08 March 2011 Supersedes 16 July 2007



NEW

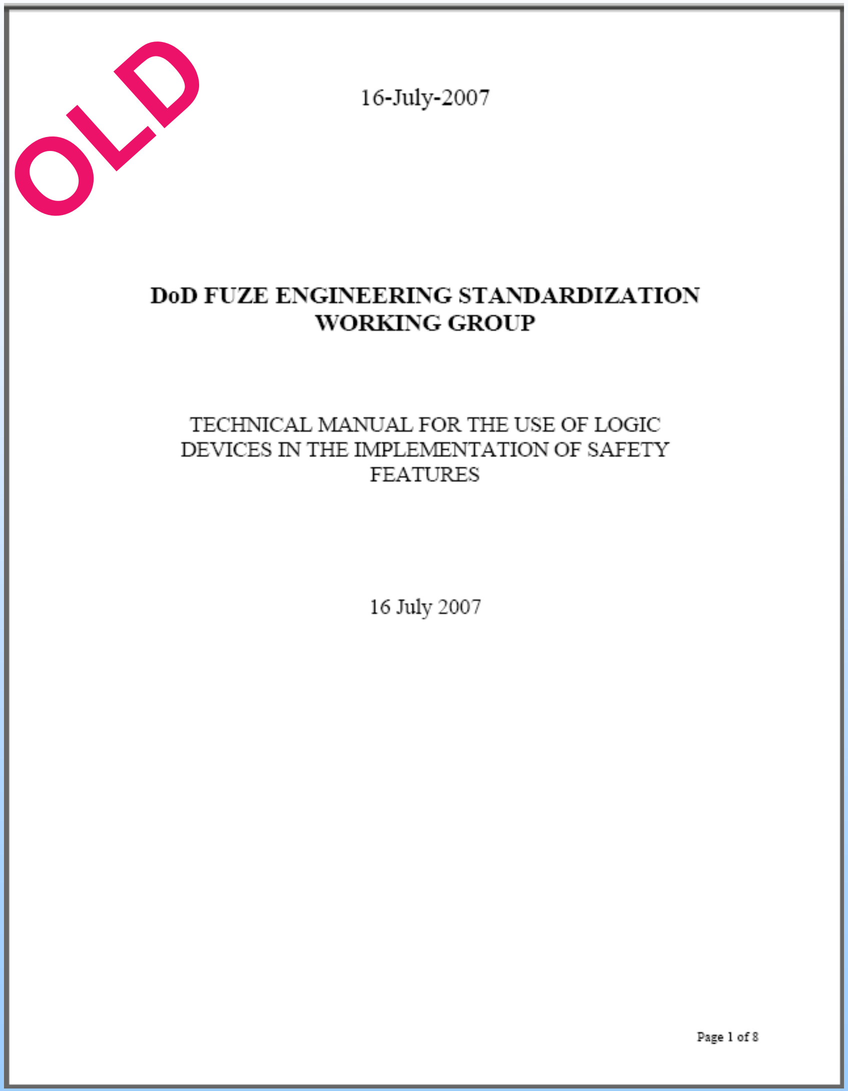
FESWG Document 2007-1

DoD FUZE ENGINEERING STANDARDIZATION WORKING GROUP

TECHNICAL MANUAL FOR THE USE OF LOGIC DEVICES IN SAFETY FEATURES

08 March 2011

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited.



OLD

16-July-2007

DoD FUZE ENGINEERING STANDARDIZATION WORKING GROUP

TECHNICAL MANUAL FOR THE USE OF LOGIC DEVICES IN THE IMPLEMENTATION OF SAFETY FEATURES

16 July 2007

Page 1 of 8

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.
- Defines Appendix A (guidelines) and B (definitions)

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited

Updated Requirements

2. OLD -> All logic devices used in the safety feature shall be non-reconfigurable.

2. NEW -> While fixed-in-structure devices are acceptable and preferred, to avoid degradation of a safety feature, any logic device used in the implementation of that feature:

a. Shall not be re-programmable.

b. Shall not be alterable by credible environments.

c. Shall not have the SF logic configuration reside on volatile memory.

d. Should be rated to meet or exceed the lifecycle environments of the system. Shall have engineering rationale provided and associated risk(s) for logic devices not rated to meet or exceed the lifecycle of the system.

Updated Requirements

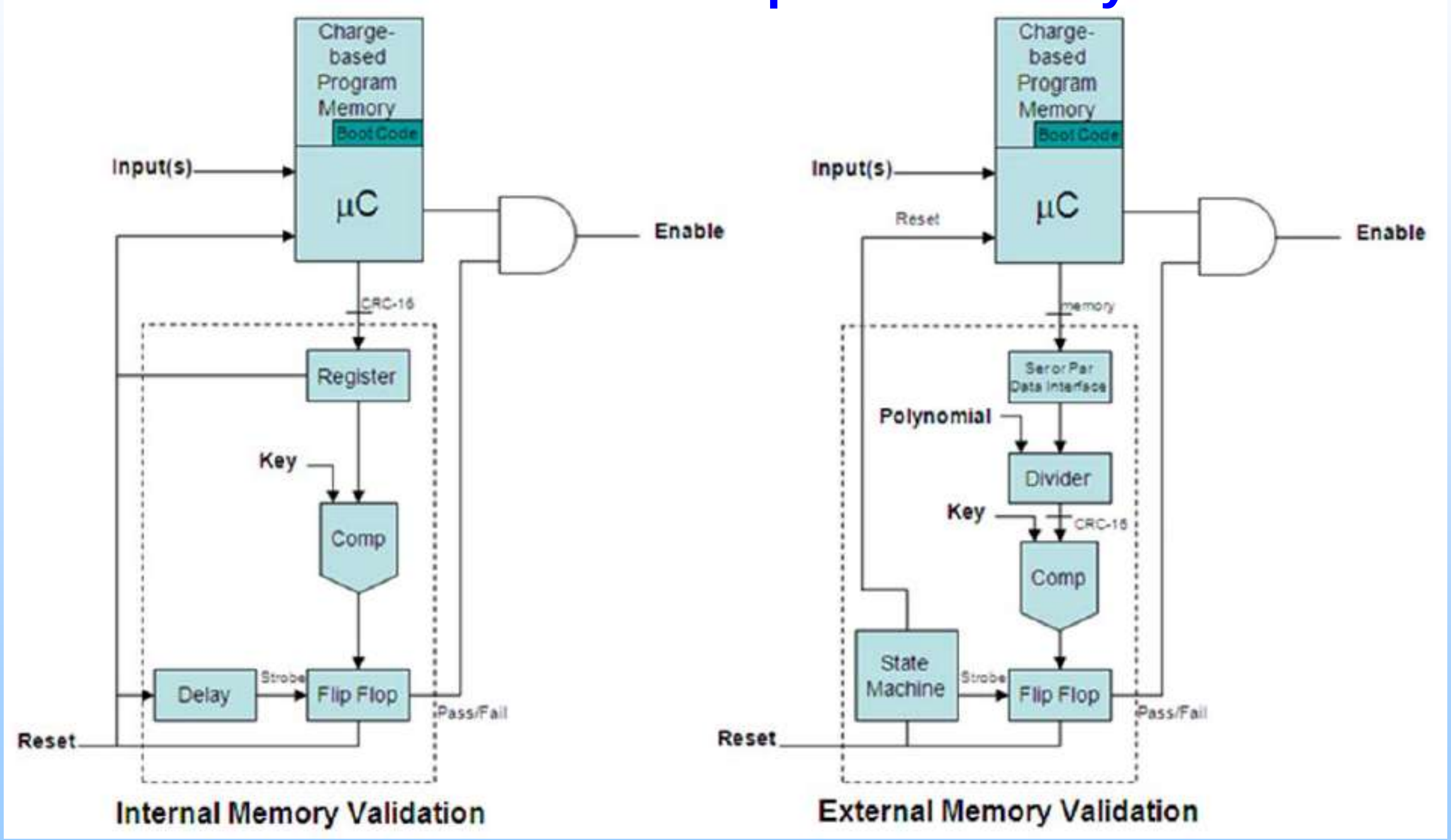
2. Cont'd

- If charged based memory is used then following shall apply:
  - Memory validation shall be performed prior to safety function
  - Validation shall have minimum rigor of CRC16
  - Computed result shall be compared externally
  - External devices shall be dedicated, fixed-in-structure, and not contain and be exclusive from any other functions.
- Consult with the appropriate Service Safety Authority for guidance.

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited

Updated Requirements

2. Cont'd - Notional example of memory validation:



Internal Memory Validation

External Memory Validation

Updated Requirements

5. During and after exposure to power transfers, transitions, and/or transients, logic devices shall not operate in a manner that results in degradation of SF.
   - 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.
   - Includes reset functions [deleted reset function requirement #13 since it's covered here]

Updated Requirements

Separated arming delay (new #7) from timing functions

6. Timing functions, excluding arming delay, within logic shall not be susceptible to single point or common cause failures resulting in early arming.
   - Requires independent timing with dissimilar technology or verification of the clocks with a known timed event.

7. Arming Delay single point and common cause failures shall be reduced to a minimum
   - Failures shall exist only at or near the expiration of the intended arming delay
   - Independent timers preferred
   - Shortest arm delay set in hardware should be set to the maximum practical value
   - Transmissions and validations of arm times should be robust (checksum, parity, CRC)

Deleted Requirement

Covered by requirement #5 so verbiage added to A.5

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.

Moved

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.

No Change

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**

No Change

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited

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.

No Change

Requirements

8. (OLD #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.

9. (OLD #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.

No Change

Requirements

10. (OLD #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.

11. (OLD #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.

No Change

Requirements

12. (OLD #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.

No Change

13. (OLD #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.

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited

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

No Change

- 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: RDAR-MEF-F
Picatinny Arsenal, NJ 07806-5000

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited

Questions???

Comments??

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited