U.S.NRC

United States Nuclear Regulatory Commission

Protecting People and the Environment

EMBEDDED DIGITAL DEVICE ISSUE IN PLANT SAFETY AND DESIGN CERTIFICATION

Eugene O. Eagle Jr.
Office of New Reactors
November 2013

Session Agenda

- Definition of an Embedded Digital Device
- Introduction
- Scope of the Embedded Digital Device Issue
- Firmware Devices
- Guidance for Applicants and Licensees
- Summary

Session Purpose

Define and clarify what constitutes an embedded digital device and the scope of the issue.

Clarify the NRC’s technical position on existing regulatory requirements for the quality and reliability equipment, including I&C, with embedded digital devices

Raise awareness that there may be potential safety issues in equipment with embedded digital devices

Definition of an Embedded Digital Device

- For the purposes of this presentation, an embedded digital device is defined as a component consisting of one or more digital electronic parts that use software, software-developed firmware, or software-developed logic that is integrated into plant equipment

Introduction

- Nuclear facilities have increased the use and reliance upon digital technology that has resulted in both benefits and challenges

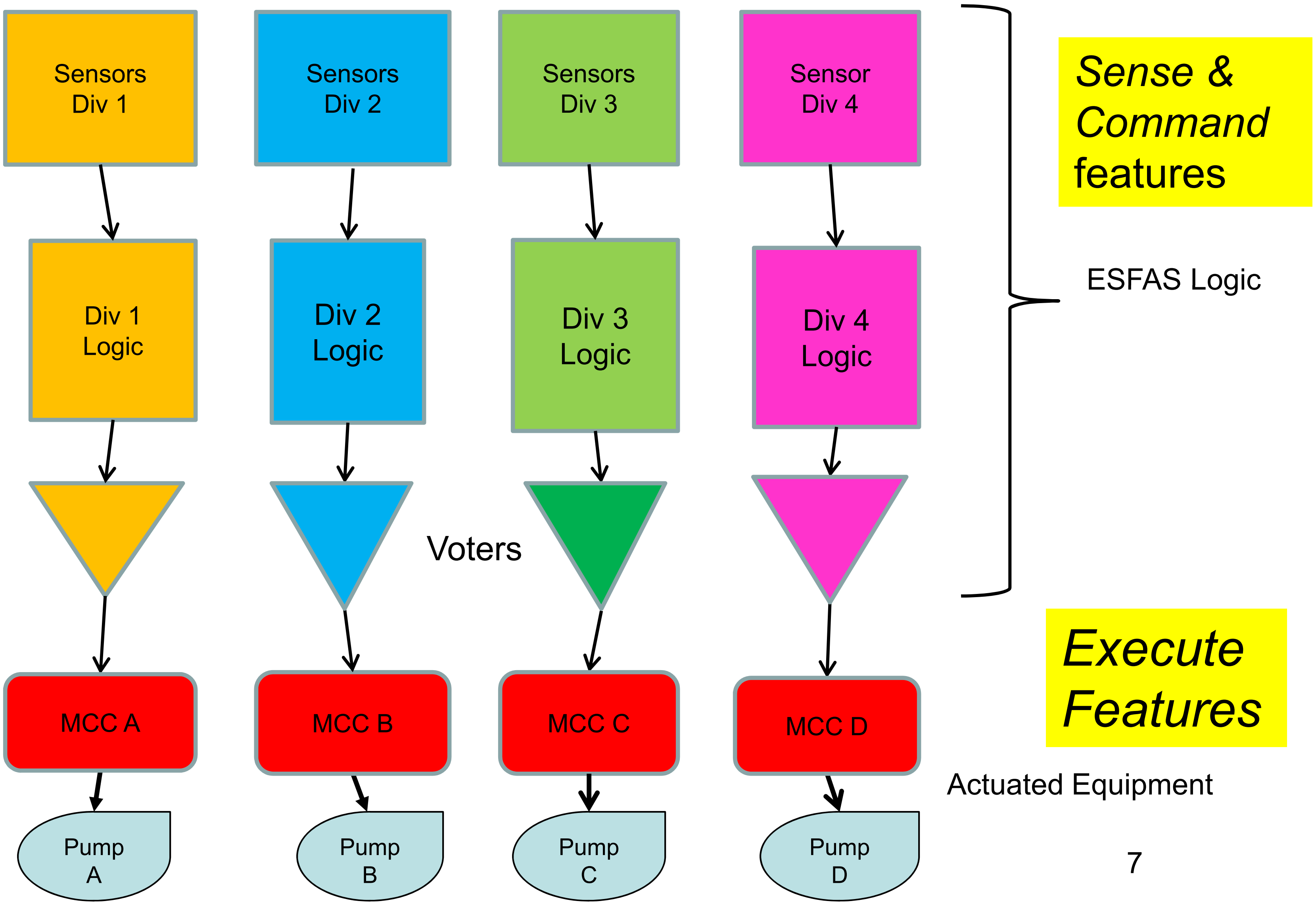
- Many types of plant equipment may now include embedded digital devices
  - Such as pumps, valves, breakers, relays, diesel generators, uninterruptible power supplies, priority logic modules

- Inclusion of these devices is not always 'advertised' by equipment vendors

Scope of Embedded Digital Device Issue

- If an embedded digital device performs (or supports) a safety function, then it should be treated consistent with regulations and guidance associated with such systems
- Non-safety related embedded digital devices should be incorporated into a plant hazards analysis

ESFAS Logic & Actuated Pumps



Sensors Div 1

Sensors Div 2

Sensors Div 3

Sensor Div 4

Sense & Command features

Div 1 Logic

Div 2 Logic

Div 3 Logic

Div 4 Logic

ESFAS Logic

Voters

MCC A

MCC B

MCC C

MCC D

Execute Features

Actuated Equipment

Pump A

Pump B

Pump C

Pump D

Firmware Devices

- Definition presented earlier for an embedded digital device includes:
  - Many digital components with executable code or software-developed logic that is permanent or semi-permanently installed within the device
  - Referred to commonly as firmware or firmware devices

- Some examples of firmware devices:
  - PLDs, FPGAs, ASICs, EPROMs, EEPROMs, CPLDs

- Devices vary widely in terms of functionality, complexity and testability

Firmware Devices

The NRC staff guidance does not accept these firmware type devices as strictly hardware components.

The NRC staff regulations and guidance do not accept the concept that licensee and applicants are exempt from responsibility for awareness of any potential safety vulnerability from embedded digital devices in procured equipment, just because they are firmware devices.

The NRC staff provides guidance (e.g., BTP 7-19, Revision 6, now incorporated in DSRS Section 7.1.5) that is helpful in considering equipment with embedded digital devices containing software, firmware, and logic developed from software-based development systems.

Guidance for Applicants and Licensees

- Licensees/applicants obtaining items and equipment from vendors that includes components with embedded digital devices should:
  - In early stages fully understand challenges that embedded digital devices may pose
  - Include in specifications for vendors, requirements to identify the use of embedded digital devices consistent with the safety significance of the equipment
  - Include in specifications requirements for the vendor to document the quality of items with embedded digital devices in a manner sufficient to support commercial grade item dedication consistent with the safety significance of the equipment

Summary

- In the early stages of their design efforts, vendors, licensees, and applicants should fully understand the challenges that embedded digital devices may pose.

- Plant equipment that include components with embedded digital devices must satisfy regulatory requirements, including quality and reliability, consistent with the safety significance of the equipment

- Procurement activities, including the commercial-grade item dedication processes, should be sufficient to ensure adequate quality

Questions

Acronyms

- ASIC - Application-specific integrated circuits
- BTP – Branch Technical Positions
- CCF – Common Cause Failure (software)
- CFR – Code of Federal Regulations
- D3 – Diversity and Defense-in-Depth
- EEPROM – Electrically erasable programmable read only memory
- EMC – Electromagnetic Compatibility
- EPROM - Erasable programmable read only memory
- ESF – Engineered Safety Features
- FPGA - Field programmable gate arrays
- HA - Hazard Analysis
- I&C - Instrumentation and Controls
- ISG – Interim Staff Guidance
- NPP - Nuclear Power Plant
- PLD - Programmable logic device
- RIS - Regulatory Issue Summary
- SMR – Small Modular Reactor