


RIC 2014
Digital Instrumentation and Controls:
Considerations of Embedded Digital
Technology
in Plant Equipment

Embedded Digital Devices
Identification and Coping




March 12, 2014
Bob Hirmanpour, PMP

Embedded Digital - Challenges


- With advent of processors and digital devices, nuclear plant instrumentation and controls components/ systems have evolved and use of embedded digital has increased.
- Industry and regulatory guidance has also evolved but focus has been on large, safety related systems.
- Components with embedded digital technology introduces different attributes that require additional guidance by the industry.

Industry needs to develop standard guidance RLH2



Step 1:

Recognition




Slide 2

RLH2 Deleted "for coping" here because coping is assumed by the NRC staff to mean that we did a D3 analysis, and that is not the intent, the intent of the guidance will be to determine if any new Hazard exists, if it does and cannot be addressed then coping is always required, but only if the Hazard exists.
Raymond Herb, 2/26/2014


Embedded Digital - Recognition

- Embedded digital technology is introduced through three primary means:
 - Design changes
 - Parts replacements / equivalency evaluations
 - Procurement
- Primary focus to date has been on microprocessor based system using software during operations.




Embedded Digital - Recognition

- Industry and the licensees need to develop processes and training to raise awareness and to recognize when components with embedded digital are being introduced.
- This includes recognition of other digital components that are not software driven in the conventional sense:
 - Field Programmable Arrays (FPGA)
 - Application Specific Integrated Circuits (ASICs)
 - Complex Programmable Logic Devices (CPLD)




Step 2:

Resolution



Embedded Digital - Resolution


- Increase awareness of the need to identify embedded digital devices in the components
 - Example, via training and process improvements
- Recognition that the requirements for embedded digital devices are no different than any other digital upgrade or change
- Evaluate the Hazards of the digital device with respect to safe plant operation



Embedded Digital - Resolution

Needed Technical / Engineering Guidance:


- Current regulatory requirements address coping with common cause failure of significant safety systems such as digital Reactor Trip System and Engineered Safety Features (e.g., GDC 22, BTP 7-19).
- Industry is working with EPRI and NEI to develop guidance to evaluate the specific hazards associated with use of digital systems.



Embedded Digital - Resolution

Preliminary Failure Analysis:

- Perform failure modes analysis of embedded digital components / system using currently approved methods and processes.
- Consider new failure modes and their effects (system hazards) due to digital nature of the devices / components/ systems.
- Mitigate undesirable effects / hazards using different design or solution.




Slide 7

B1 I wouldn't say this. It contradicts the feedback that we provided the NRC on hte RIS.
BYRJC, 3/5/2014

Embedded Digital - Resolution

Common Cause Failure Analysis:


- Include considerations for Common Cause Failure susceptibility analysis as appropriate.
- The level and depth of the analysis should be commensurate with:
 - Level of safety
 - Complexity of the system




Embedded Digital - Resolution

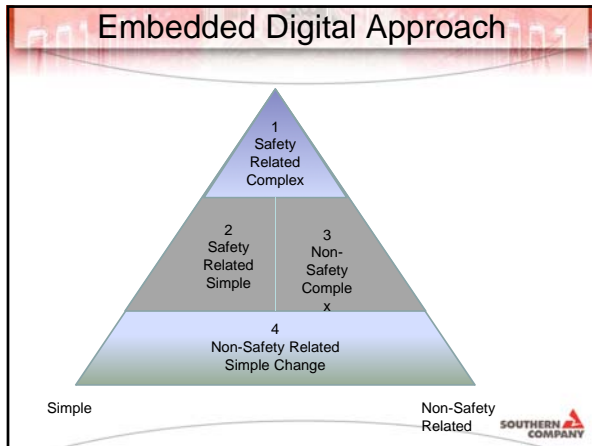
Mitigation:

- Establish mitigation strategy during early stages of design to eliminate undesirable system hazards, examples:
 - Diversity
 - Use of different technology
 - Segmentation



Potential Solution






- ### Embedded Digital Approach
1. Safety Related – Complex (e.g., Reactor Trip System)
 - Regulatory Based
 - Diversity and Defense in Depth analysis
 - Diverse Actuation System
 - Best Estimate
 2. Safety Related – Simple (e.g., transmitter)
 - Appendix B
 - Failure Mode and Hazards Analysis
 - 100% Testing
- SOUTHERN COMPANY

- ### Embedded Digital Approach
3. Non-Safety Related – Complex or Critical Systems (e.g., Plant Controls, Multiple Systems)
 - Common Cause Failure Considerations
 - Failure Mode and Hazard Analysis
 - Engineering Solutions
 4. Non-Safety Related – Simple
 - No special consideration, use standard processes
 - Multiple changes should be treated as 3 above
- SOUTHERN COMPANY

Embedded Digital Approach

Procurement

- Enhance processes and train procurement engineers / staff on special requirements for embedded digital
- Ensure digital requirements are passed to vendors / sub-vendors
- Ensure equivalency evolutions (form-fit-function) include special considerations for embedded digital



Questions?

