JENSEN HUGHES

Advancing the Science of Safety

ADVANCED TECHNIQUES FOR MODELING FIRE-INDUCED CIRCUIT FAILURES OF DIGITAL CONTROL SYSTEMS IN SUPPORT OF FIRE PROBABILISTIC RISK ASSESSMENTS

Nicholas Lovelace

9/28/2017

OVERVIEW

TOPIC FOR PRESENTATION OR AGENDA

- Introduction
- Circuit Analysis Methods
  - Black Box
  - Signal
  - Functional
- Conclusion & Questions

INTRODUCTION

- Digital control circuits are becoming more prevalent for usage in Nuclear Power Plant's (NPP's), however there is currently little industry and regulatory guidance available for modeling and circuit analyzing these control circuits for a Fire PRA.
- Digital control systems have the potential to introduce new fire – induced failure modes or associated circuit concerns that were not traditionally seen in the analog control systems.
  - Logic modeling for probabilistic risk models are typically done at a high level based on applicable failure data, this does not typically capture the fire-induced failures in a manner conducive to producing realistic results.
  - Logic models can require extensive changes due to circuit analysis and modeling boundary differences.
  - Signals may be processed through multiple communication and hardware devices, causing difficulties to pinpoint all devices that can cause fire-induced failure of the digital system

INTRODUCTION

Continued...

- Fire-induced failure from common power supply concerns. Inputs or outputs may not be isolated between individual signals.
- Difficult to tell how feedback inputs from controlled components are utilized by the digital control system. Do they provide indication of component status or are they interlocks.
- Digital hardware may be used to process and send both manual and automatic signals to plant components for operation, causing modeling difficulties for implementing Fire PRA operator actions.
- Digital circuits can be susceptible to smoke and heat at lower thresholds than traditional analog circuits (i.e. sensitive electronic)

CIRCUIT ANALYSIS METHODS

- Black Box Circuit Analysis
  - This approach is the simplest form to capture fire-induced failures.
  - Essentially cable selection versus circuit analysis.
  - Physical location of all devices and cables needed for the digital control system operation.
  - This approach is generally conservative. Works for NPP's with minimal digital control systems (i.e. retrofits).
  - Not well suited for NPP's with significant digital control systems.
  - Potential to miss unique failure modes or physical locations that the signal is susceptible to fire damage in the analysis if all of the required digital control system devices are not all captured modeling.

CIRCUIT ANALYSIS METHODS

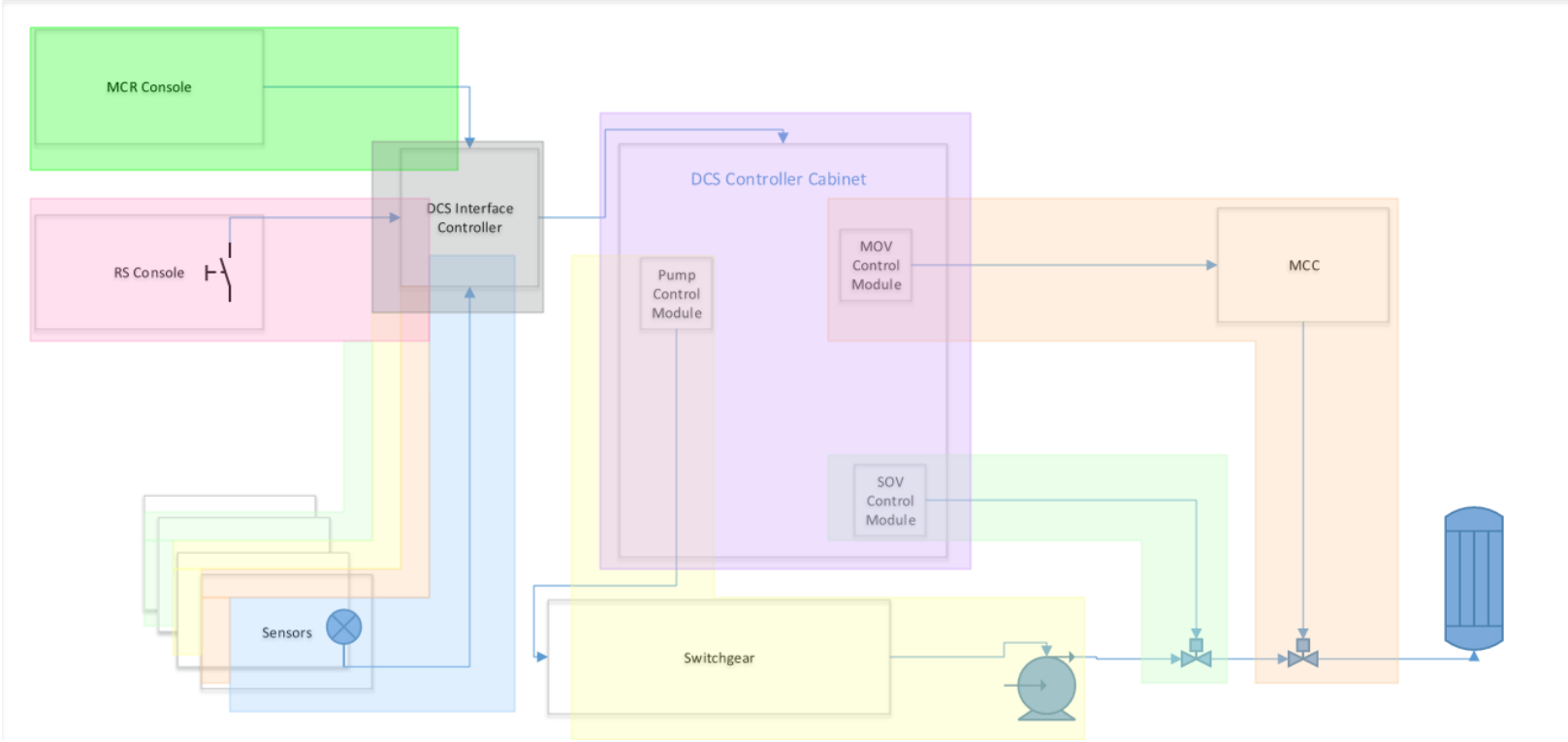
- Signal Circuit Analysis
  - This approach essentially reproduces the digital control system programming logic for every required signal into the Fire PRA model.
  - The appropriate cables, components, power supplies, and other dependencies are mapped to each modeled logic event.
  - Potential to require significant modeling effort to add the logic in the PRA model and mapping to logic events.
  - Potential to miss fire-induced failures or common power supply concerns if not isolated, by focusing only on the logic and not the electrical circuits.

CIRCUIT ANALYSIS METHODS

- Functional Circuit Analysis
  - This approach is a blend of the black box and signal analyses.
  - Best to start with the end component and work backwards through the digital control logic to map out the required signals and screen out any non-required control signal paths.
  - Circuit boundaries should be developed as sets of pseudo components. The boundaries of each pseudo should be based on spatial characteristics of the digital control circuits for the desired logic functions, but physical boundaries will overlap.
  - Typically involves less model changes, since only the pseudo components and power supplies need to be modeled.
  - One of the keys to the pseudo boundary is to avoid combining any cross divisional cables, devices, or signals.
  - Approach takes more upfront planning by experienced systems and circuit analysts.

CIRCUIT ANALYSIS METHODS

EXAMPLE FUNCTIONAL CIRCUIT ANALYSIS BOUNDARY BREAKDOWN



CONCLUSION

SUMMARY OF PRESENTATION

- A “one-size fits all” approach for performing Fire PRA modeling and circuit analysis for digital control circuits is not appropriate
- Fire PRA results are highly dependent on the circuit and logic design of the digital control system. Knowing how it is designed to function and how it was built (implemented) are both important.
- Screen non-required signals or functions first, then develop pseudo boundaries.
- Watch out for associated circuit concerns and cross divisional failures.

QUESTIONS?

Contact

Nicholas Lovelace
+1 402-540-4783
nlovelace@jensenhughes.com

For More Information Visit
www.jensenhughes.com

JENSEN HUGHES
Advancing the Science of Safety