Common Cause Modeling

Huntsville Society of Reliability Engineers
RAM VIII Training Summit
November 3-4, 2015

Frank Hark Bastion Technologies, Inc.
Paul Britton, NASA
Robert Ring, Bastion Technologies, Inc.
Steven Novack, Bastion Technologies, Inc.
Agenda

- Objective
- Key Definitions
- Calculating Common Cause
- Examples
- Defense against Common Cause
- Impact of varied CCF and abortability
- Response Surface for various CCF Beta
- Takeaways
Objective

- Common Cause Failures (CCFs) are known and documented phenomenon that limit the benefit of system redundancy as a design approach to achieve high reliability.

- Because Launch vehicle data is sparse, generic data from the nuclear industry is used to estimate CCF for launch vehicles.

- This presentation addresses the impact of CCF risk on system reliability and safety.
Key Definitions

- A common cause failure (CCF) is a failure where:
  - Two or more items fail within the mission time from a common failure mechanism.

- Beta Factor is defined as the fraction of the component failures that result in a common cause failure.
CCFs may also be viewed as being caused by the presence of two factors:

1. Root or proximate Cause, i.e., the reason (or reasons) for failure of each component that failed in the CCF event, and a
2. Coupling Factor (or factors) that was responsible for the involvement of multiple components.

\[ \beta = \frac{\lambda_C}{\lambda_T} \Rightarrow \lambda_C = \beta \lambda_T; \]

\[ \lambda_I = (1 - \beta)\lambda_T \]

CC Basic Events account for all common causes not explicitly modeled in the fault tree.
The following are examples of actual CCF events:

- Hydrazine leaks leading to two APU explosions on Space Shuttle mission STS-9
- Multiple engine failures on aircraft (Fokker F27 – 1997, 1988; Boeing 747, 1992)
- Three hydraulic system failures following Engine # 2 failure on a DC-10, 1989
- Failure of all three redundant auxiliary feed-water pumps at Three Mile Island NPP
- Failure of two Space Shuttle Main Engine (SSME) controllers on two separate engines when a wire short occurred
- Failure of two O-rings, causing hot gas blow-by in a solid rocket booster of Space Shuttle flight 51L
- Failure of two redundant circuit boards due to electro-static shock by a technician during replacement of an adjacent unit
- A worker accidentally tripping two redundant pumps by placing a ladder near pump motors to paint the ceiling at a nuclear power plant
- A maintenance contractor unfamiliar with component configuration putting lubricant in the motor winding of several redundant valves, making them inoperable
- Undersized motors purchased from a new vendor causing failure of four redundant cooling fans
- Check valves installed backwards, blocking flow in two redundant lines
- CCFs may also be viewed as being caused by the presence of two factors:
Reducing it

Checklist for reducing common cause categorized into 8 groups

1. Degree of physical separation/segregation
2. Diversity/redundancy (e.g., different technology, design, different maintenance personnel)
3. Complexity/maturity of design/experience
4. Use of assessments/analysis and feedback data
5. Procedures/human interface (e.g., maintenance/testing)
6. Competence/training/safety culture
7. Environmental control (e.g., temperature, humidity, personnel access)
8. Environmental testing
Impact of Varied CCF and Abortability

- CCF estimate becomes important when trading between a 1 out of 2 system and 1 component fails
  - Abort immediately or continue mission
  - STS used fail opt/fail safe redundancy
- Cost/weight concerns limit some systems to one level of redundancy
- What is the benefit of adding an additional level of redundancy
Response Surface for Various CCF Beta

Odds Against Continuing with the Mission after 1st Failure
(Contour Plot)

- **Worst**
- **Best**

1:1 (Even) 2:1 3:1 4:1 5:1

Increasing Odds Against Continuing the Mission

Example: "2:1 Against" means the crew is twice as likely to be lost by continuing the mission versus aborting the mission.

Probability of 2nd Failure Given 1st Failure

LOC Given 2nd Failure
Common cause failure is a known impact to redundant system

Common modeling assumptions may underestimate the real risks

When data is unavailable, it is important to judge the impact of system reliability, safety, and common cause factors over a range of values
