I&C Modeling Approach

- Detailed fault tree of Protection System (RPS and ESFAS)
  - Level of detail needed to show functional diversity
  - Level of detail to computer processor modules to resolve dependencies (computers are multi-tasking)
- Backup systems for D3 will be included in model
- Control System not modeled in detail; included in initiating event frequency. When operating experience is available expect reduction in initiating event frequencies

I&C Failure Data and Sources

- Manufacturers of equipment typically provide MTBF data for I&C modules from operating history, testing, or calculation
- Manufacturer's field data includes RPS/ESFAS systems operating in European
- Conservative Chi-squared (95%) treatment to bound observed failure rate

I&C CCF Modeling

- Software Development Process is Robust:
  - High quality software development process
  - Application software uses only qualified software modules from function block library
  - Deterministic operating system reduces CCF potential

- PRA treats software failure as a CCF mechanism for the computer processors
- CCF applied to computer processors that have the same application software (algorithms) and inputs
- Conservative Beta factor

Accounting for Software in PRA

- National Academy of Sciences:
  - “The committee agreed that a software failure probability can be used for the purposes of performing PRA in order to determine the relative influence of digital system failure on the overall system.”
  - “Hardware and software should be treated together as a system”
  - Recommendations emphasize diversity
- NPP PRAs:
  - Need estimates for failure/CCF probability of software that recognize differences in I&C architecture, diversity, and defensive measures.

Suggested Research

Generic SW Failure/CCF Probabilities

I&C Architecture	Defensive Measures Worse ←	→ Better
	NSR type computer: copper networks, dynamic memory allocation, synchronous	Independent channels/networks, cyclic operation, asynchronous, static memory allocation, etc.
SW on a single computer		
Identical SW on Redundant Computers -TMR/voting-same train		
-Independent trains		
Functionally diverse SW on Separate Computers		
etc		