UNITED STATES NUCLEAR REGULATORY COMMISSION

Digital Instrumentation and Control

Public Meeting of December 12, 2006:

Interchannel Communications

Setting the Focus

Objectives
and Criteria for Success

- open discussion of technical issues
- focus on safety concerns
  - focus on the independence and functionality of the safety system
  - recognize and address important nonsafety design objectives
- show how proposed designs support the safety criteria

Applicability

The term “interchannel communications” as used here includes:

- exchange of information or commands among safety channels
- exchange of information or commands in either direction between any safety channel and any non-safety channel or circuit

Fundamental Principles: *Isolation and Independence*

- nothing outside a safety channel can interfere with the channel’s safety function
  - normal operation of the external system
  - faulted operation of the external system
  - external fault propagation
- failures within the safety channel count as “single failures”

Paradigm Principles: *Functionality Allocation -- Safety Layer*

- safety functions
- minimal “housekeeping”
  - verification of safety signals
  - self-testing of safety functions
  - external communications

Paradigm Principles: *Functionality Allocation -- NonSafety Layer*

- nonsafety functions
- all system-wide functions, such as:
  - self testing of nonsafety functions & integration of safety layer self-test results
  - verification of nonsafety data
  - cross-verification of all data (on-line monitoring)
  - general data accumulation & archiving

Paradigm Principles: *the Communication Process*

- A safety processor must:
  - – never wait for any signal or condition from outside its own safety channel
  - – receive information from outside its own safety channel only through interface memory that is fully controlled by another processor
    - The interface memory and processor must be located in the same channel as the safety processor, and the safety processor must always have immediate priority for access.

Paradigm Principles: *External Influences*

- No external device can change any safety channel operating characteristic, setpoint, etc. except under controlled hardware conditions.
- An external device can provide information or requests for operation to a safety processor, provided the safety processor responds only within the context of its safety function.

What we are Looking For

demonstration that all applicable isolation and independence criteria are met