EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Staff Concerns Related to Common-Cause Failure in Digital Systems

EPRI Plan for Addressing Technical Issues

John Connelly – Ray Torok – Bruce Geddes
NEI 01-01 Focus Team
Meeting on NEI 01-01

March 5, 2014

Contents

- NRC Staff Concerns 10 and 11
- A Broader Look at CCF
- The Plan
- CCF Concepts
- Overview - CCF Issues in Digital Systems

NRC Staff Concerns
Concern #10 from NRC Letter

10) Traditional analog systems and older digital systems are typically implemented as independent systems. Digital modification can introduce interactions or couplings between previously independent systems. These couplings in non-safety-related systems can also have an impact on the assumptions in the accident analyses. NEI 01-01 does not include guidance to address increases in coupling/ interaction or decreases in independence.

Underlying concerns:

Potential CCF introduced by new couplings or interactions

NRC Staff Concerns
Concern #11 from NRC Letter

11) Traditional analog systems have failure behaviors that are easier to characterize than complex digital systems. NEI 01-01 does not provide guidance for how to address the failure characterization of digital systems. That is, it is possible to design a single computer controlled system to control equipment associated with several functions. Is it necessary to assume the spurious actuation of all controlled components, in the worst possible way at the worst possible time? Why or why not?

Underlying concerns:

Potential CCF introduced by combining control functions

Multiple spurious actuations that create unanalyzed events

A Broader Look -
We Plan to Address CCF in all these Contexts

Issues pertinent to Concerns #10 & #11:

- Combining functions in a single controller
- Combining controls for multiple systems on a single platform
- Concurrent spurious actuations of multiple control functions that create unanalyzed events
- Multiple systems with identical platforms or software elements
- Non-safety systems with internal redundancy that share resources (e.g., power supplies, timing signals, etc.)
- Multiple plant systems or controllers that share resources (e.g., data networks)

In addition:

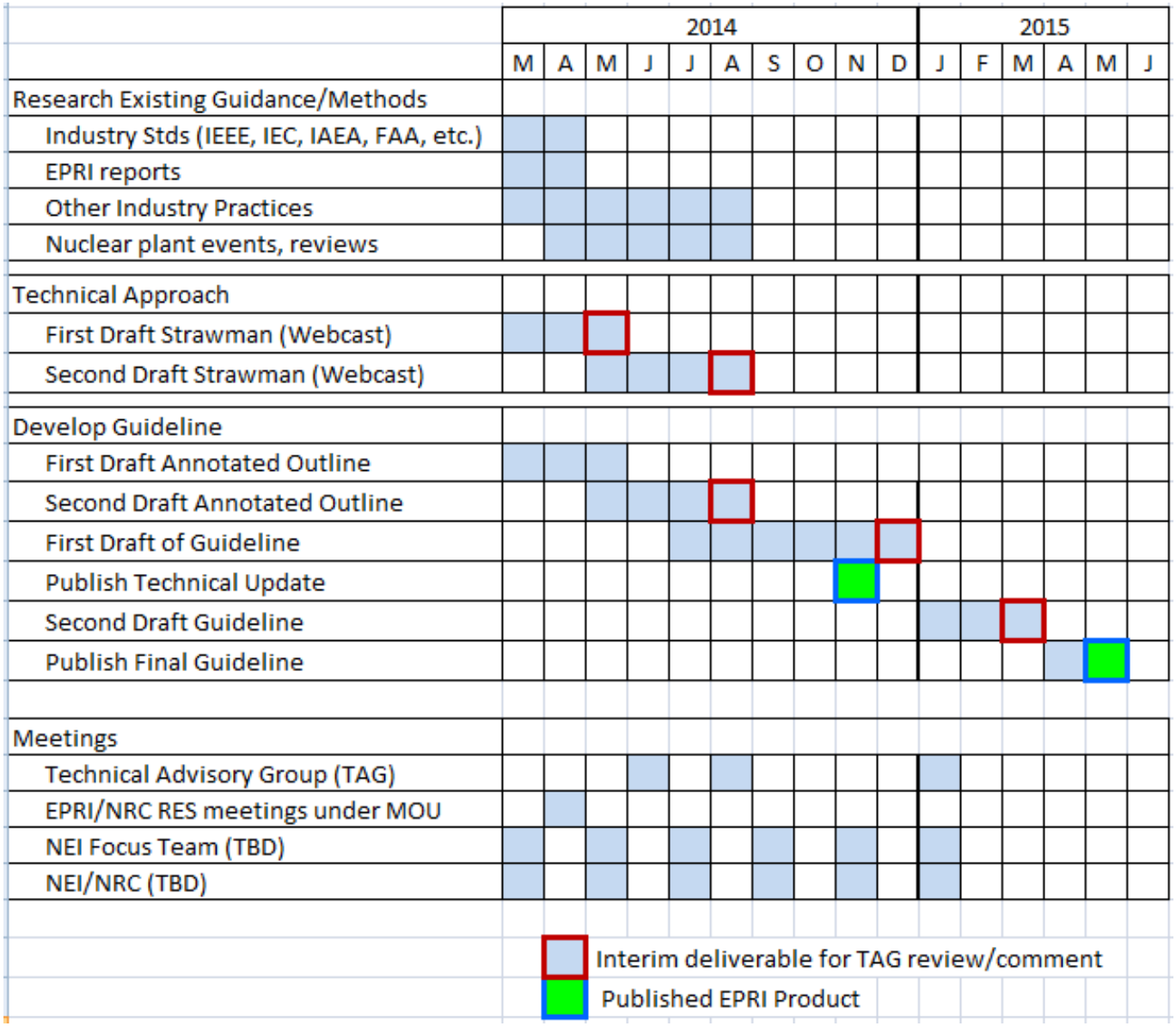
- Redundant divisions of identical equipment/software

Note: This is a global technical issue, not just a U.S. regulatory issue. It applies to all operating and new plants worldwide

The Plan –
EPRI Project to Develop Guidance Document

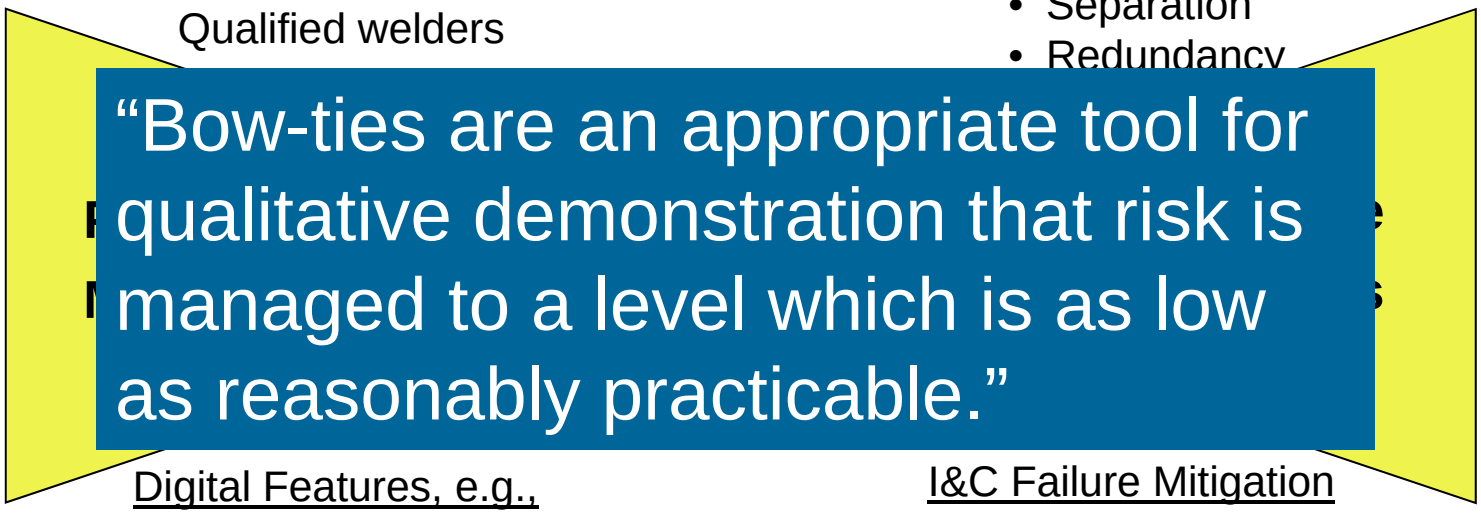
- Target audience:
  - Utility I&C design engineers, 50.59 evaluators, safety analysis engineers, licensing engineers, PRA analysts
- Utility Technical Advisory Group (TAG) input/oversight
- Process for applying the new CCF guidance
  - Apply in design activities
    - Assess susceptibility to digital failure and CCF early in design
    - Help identify and address vulnerabilities
    - Develop design criteria to avoid CCFs
  - Training and industry workshops to communicate approach
  - Results support 10 CFR 50.59 reviews
- Guidance also provides technical basis for NEI Focus Team effort to resolve NEI 01-01 concerns

The Plan, cont'd – Draft Schedule and Milestones



EPRI ELECTRIC POWER RESEARCH INSTITUTE

Protection includes both Prevention (Avoidance) and Mitigation - The "Bow-Tie Diagram"



Causes

Consequences

Piping Attributes, e.g.,
- Qualified materials
- ASME code
- Inspections
- Qualified welders

Piping Failure Mitigation
- Non-safety backups
- Operator action
- RPS/ESFAS
  - Separation
  - Redundancy

"Bow-ties are an appropriate tool for qualitative demonstration that risk is managed to a level which is as low as reasonably practicable."

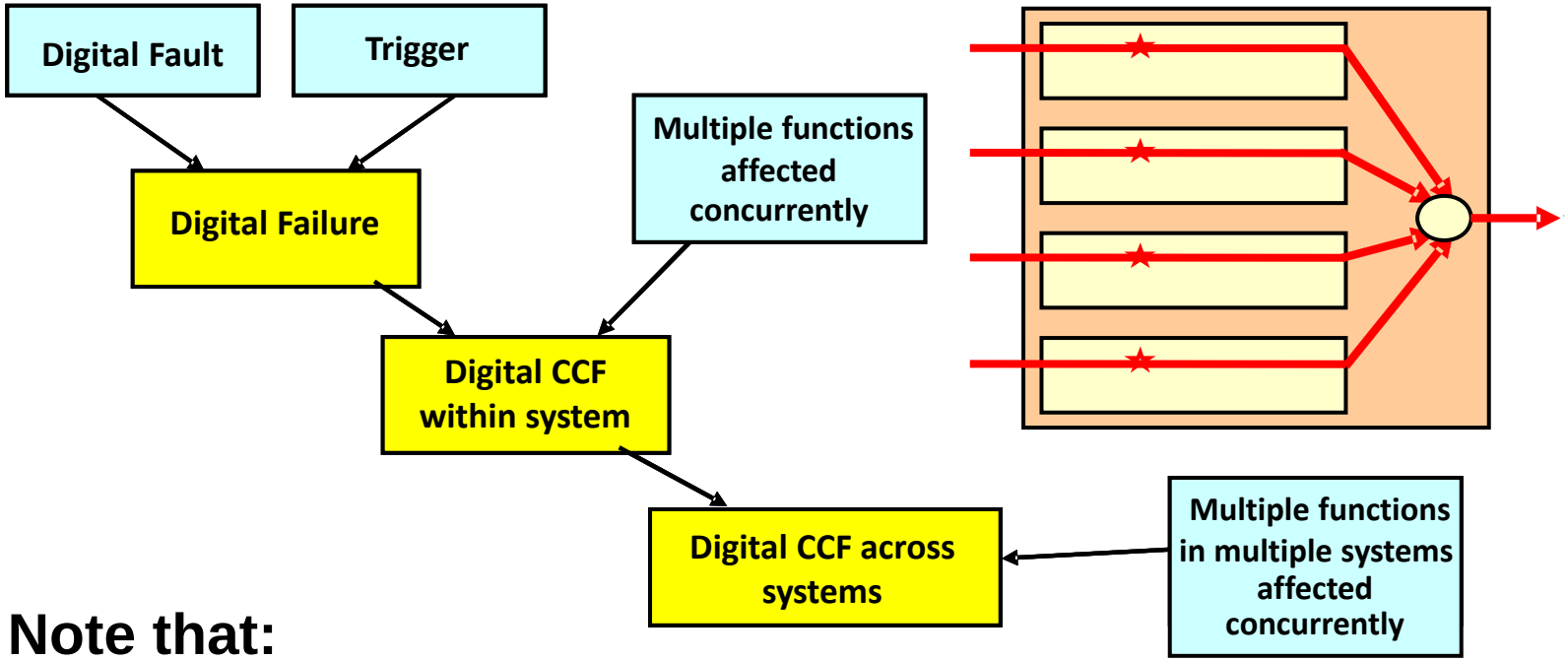
Digital Features, e.g.,
- Watchdog timers
- Data validation
- Cyclic processing
- Minimal interrupts
- Functional diversity
- Segmentation

I&C Failure Mitigation
- Reactor trip
- Non-safety control actions
- Operator action
- Diverse actuation for RPS & ESFAS
- …

Approach, cont'd –
Draw From and Expand Existing Guidance on CCF

- Consider all types of CCF and all contributors to protect against functional failure – both avoid and mitigate, including:
  - Traditional hardware practices - quality assurance, qualification testing, etc.
  - Defensive design measures in software, hardware, architecture, procedures, operation, etc.
  - Failure analysis
  - Test coverage
  - Performance records
  - Risk and fault tree analysis (FTA) insights
  - Mitigation mechanisms
  - Coping and safety analysis insights, including "bounding" analysis
- Identify effective failure avoidance measures
- Identify and address CCF vulnerabilities

CCF Concepts – Ingredients for Software CCF: Faults and Triggers



Note that:

- Not all digital failures become CCFs
- Not all digital failures and CCFs are safety-significant
- Defect-free software is not necessary to avoid CCFs

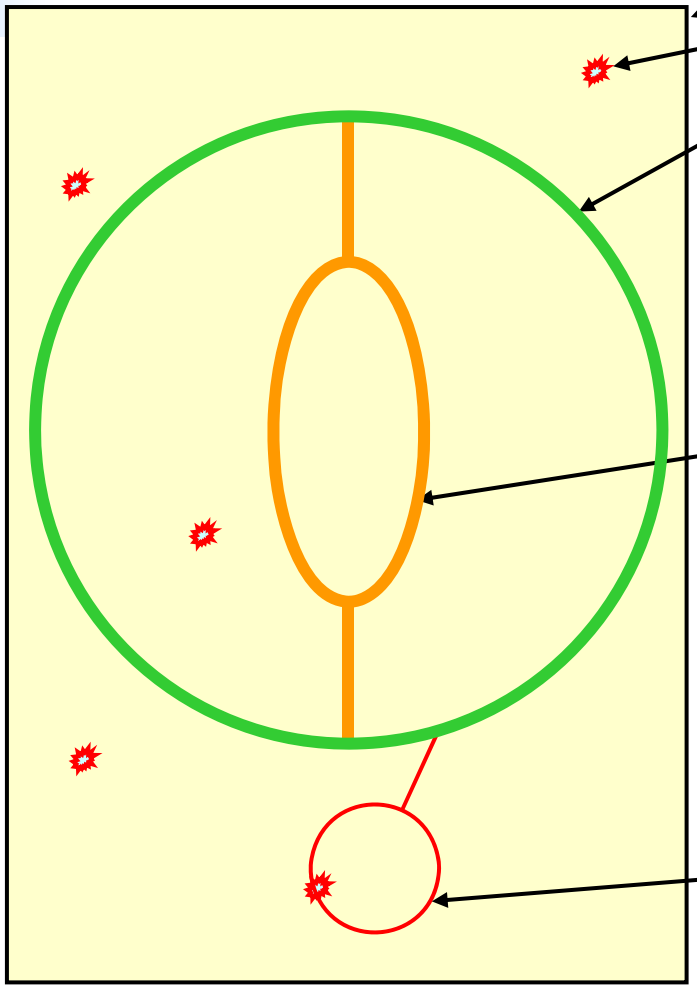
Guidance will expand on these concepts

CCF Concepts - Faults and Triggers cont'd…
CCF Likelihood (L)

- Software "failure" requires a fault (same as defect) and a trigger
- Trigger is an unanticipated, unexpected, or untested condition **(Software is very, very good in anticipated, tested conditions)**

We will include guidance on how to reduce the likelihood of faults and triggers

CCF Concepts - Example of Trigger Avoidance
System Constrained to Well Understood and Tested Trajectories



Complete domain of behavior
May contain residual digital faults

Path exercised continuously in normal situations
Influence factors during continuous operation:
- normal process inputs (validated before use)
- short-term memory (as little as possible)
- clock interrupts (thorough verification)
- (process-related interrupts: none)
- (resource management: static)

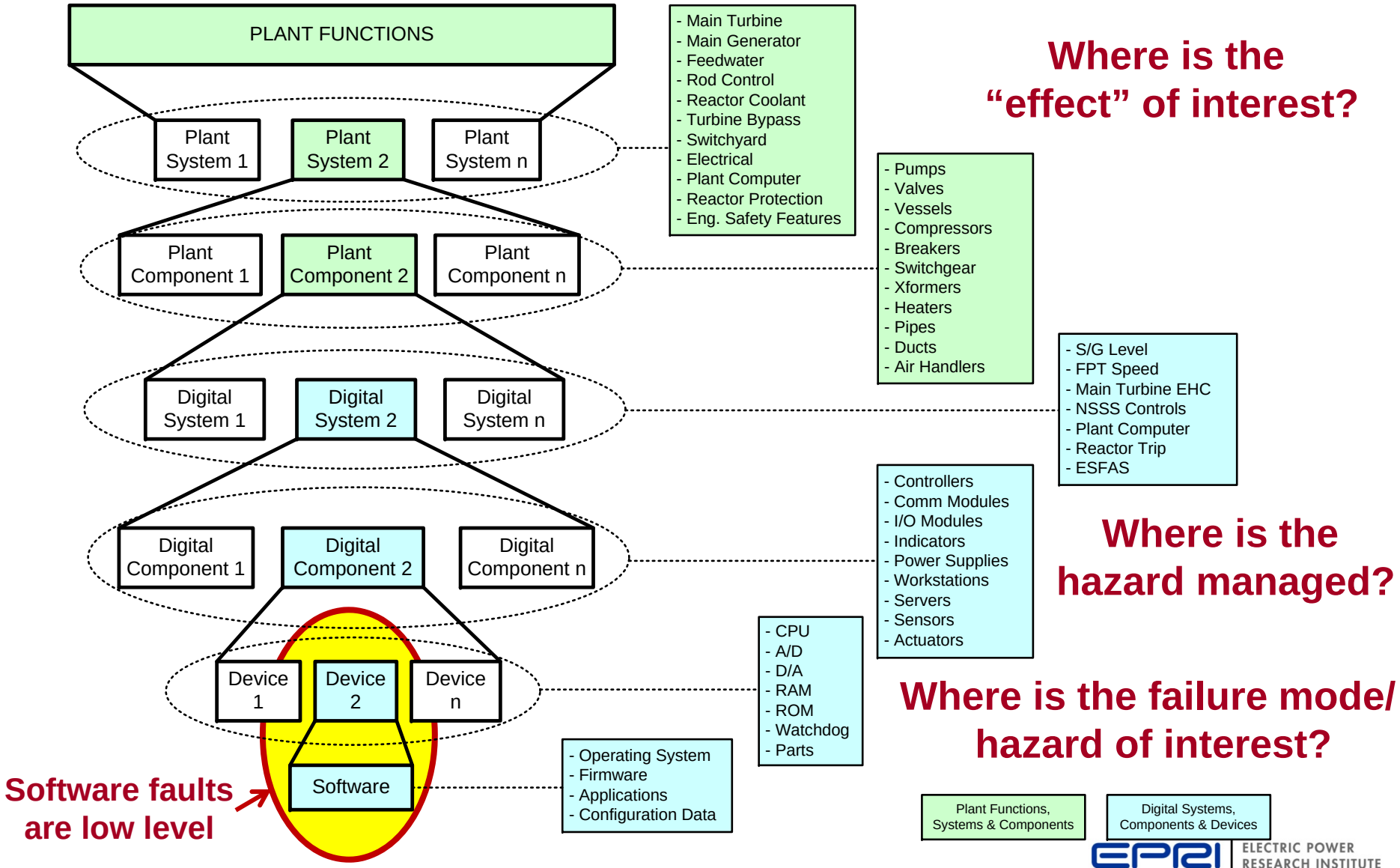
Path exercised in occasional but tested situations
Influence factors that could disrupt cyclic behavior:
- initialization (only once)
- operator requests (single channel)
- hardware failures (single channel)
- exceptions (very simple)
- codified dates & times (e.g., Y2K)
- plant transients: affect all channels

Path exercised in unanticipated or untested trajectories

The guidance will describe methods for avoiding unanticipated and untested trajectories

Concepts - Protection Against Hazards

Hazard can be Managed at Several Levels



EPRI ELECTRIC POWER RESEARCH INSTITUTE

Approach, cont'd –
Important Considerations

- If a defensive design measure that avoids a particular type of failure has been demonstrated, then that failure is unlikely
- Provisions to ensure credited defensive measures are maintained
- Credit protective (preventive and mitigative) measures both inside and outside the digital system
- Risk-benefit of additional protection ("reasonably practicable")
- Processed-based development standards
- Look at design standards (not process-based) in other industries
- CCF protection tailored based on application, complexity

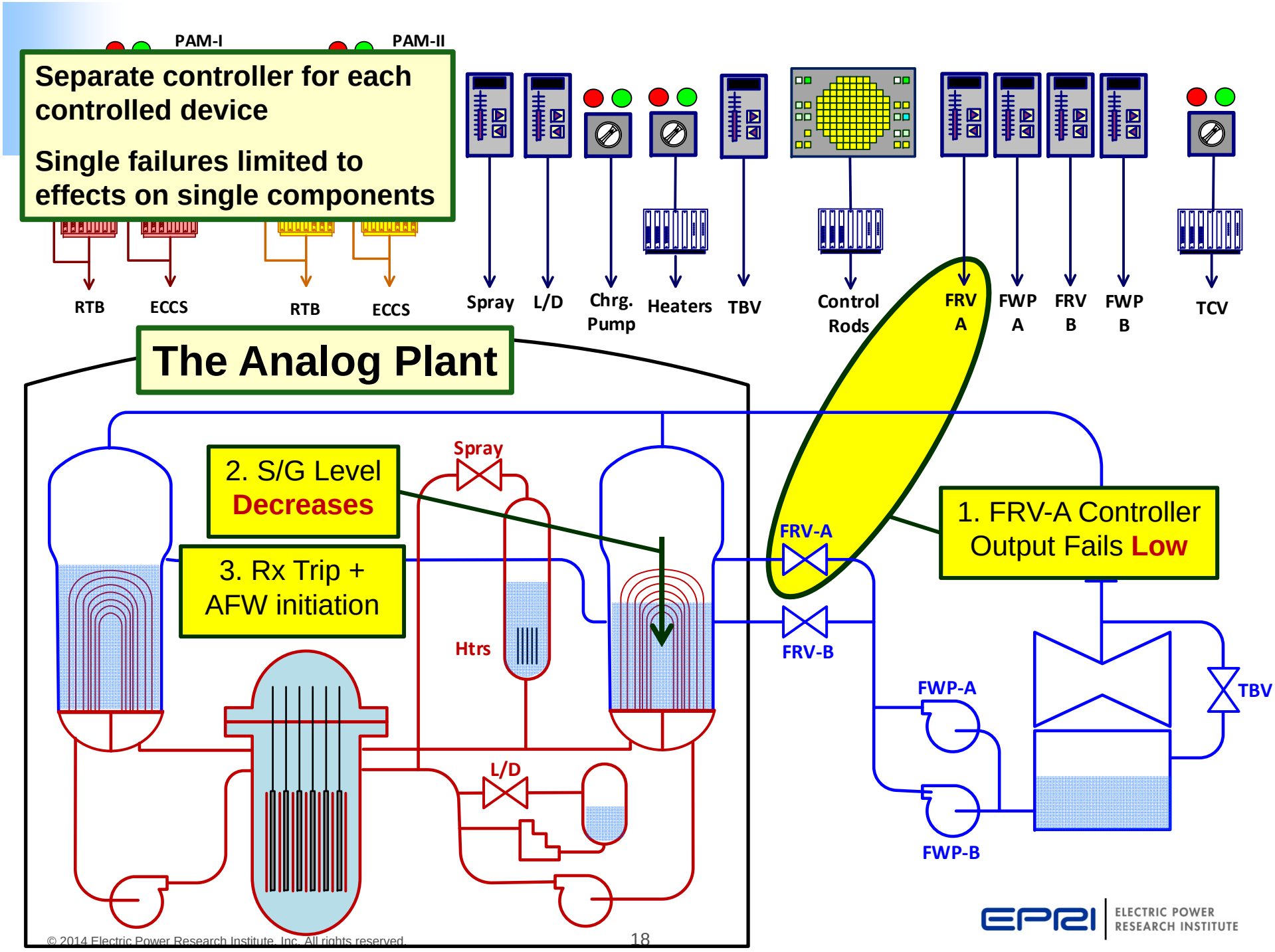
Approach, cont'd –
Important Considerations, cont'd

- Tools that reduce likelihood of software defects, e.g., static analyzers, automated design tools
- Safety vs. non-safety – dependence on process vs. design
- Coping/bounding analysis assumptions – best estimate?
- Check recommended preventive measures against OE to make sure they address known potential and actual CCFs
- Failure analysis techniques (e.g., FMEA, systems theoretic process analysis, and fault tree analysis) to:
  - identify potential CCF vulnerabilities
  - identify finite sets of combinations of spurious actions of multiple components

Summary

- EPRI project to develop CCF guidance
- Address NRC concerns 10 and 11, and broader CCF issues
- Consider both preventive and mitigative protection measures
- Target audience is utility engineers
- Periodic updates with NEI and Staff
- Technical update report late-2014, final report mid-2015
- Objectives:
  - Help utility engineers assess, manage, and reach a conclusion regarding CCF susceptibilities
  - Develop balanced prevention, mitigation and coping analysis strategies
  - Provide technical basis for resolving NEI 01-01 concerns

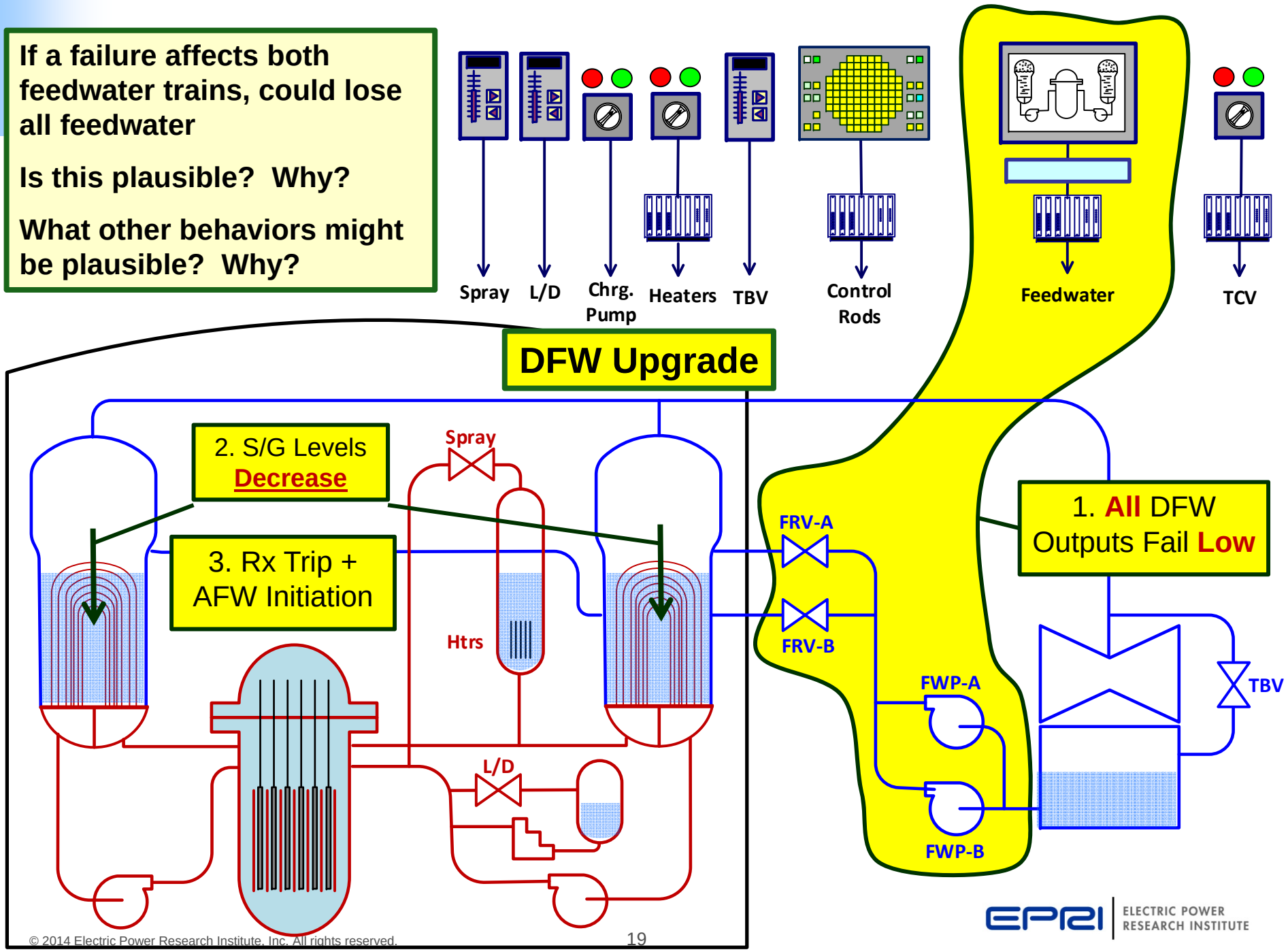
Overview - CCF Issues in Digital Systems



If a failure affects both feedwater trains, could lose all feedwater

Is this plausible? Why?

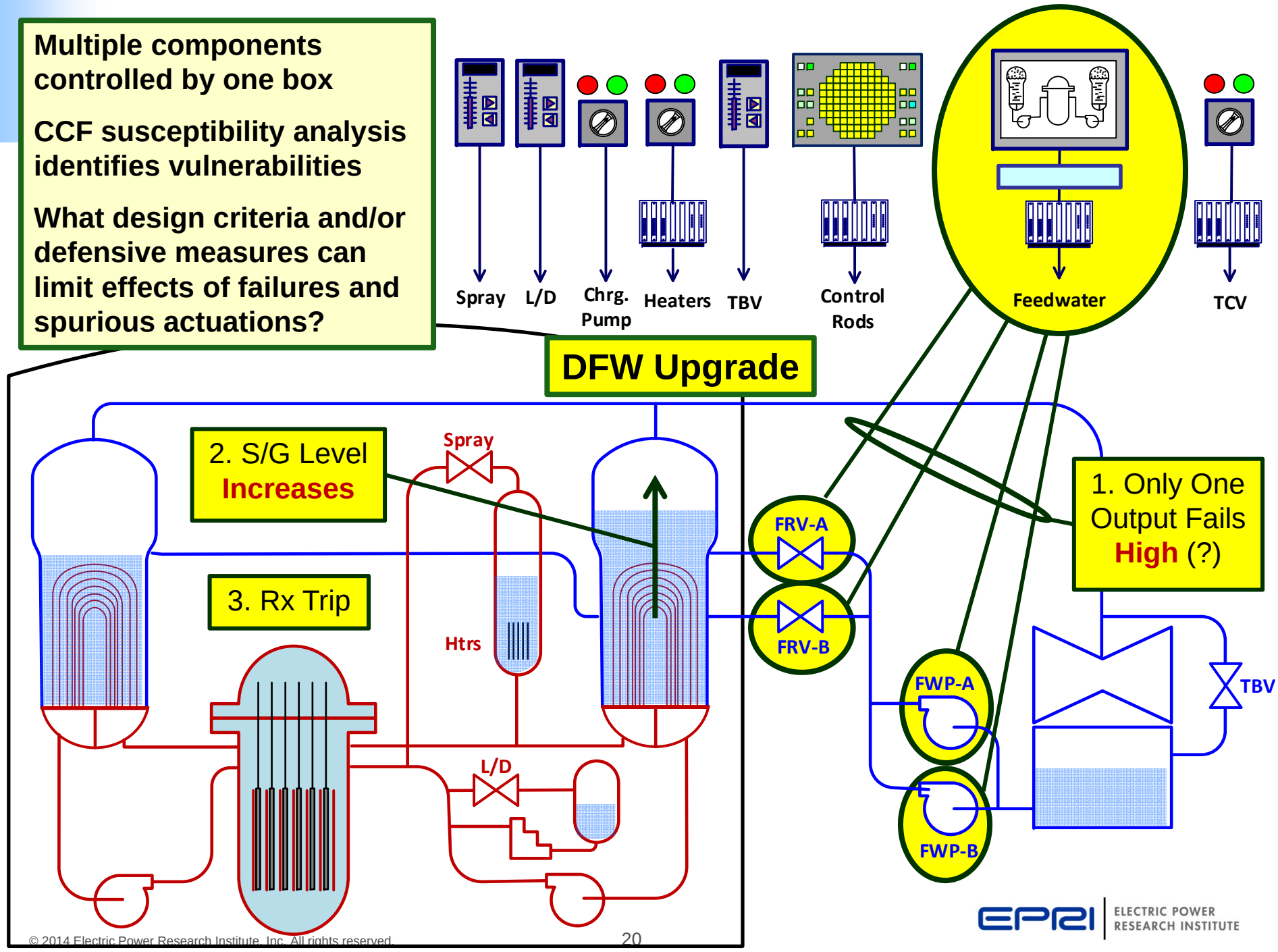
What other behaviors might be plausible? Why?



Multiple components controlled by one box

CCF susceptibility analysis identifies vulnerabilities

What design criteria and/or defensive measures can limit effects of failures and spurious actuations?

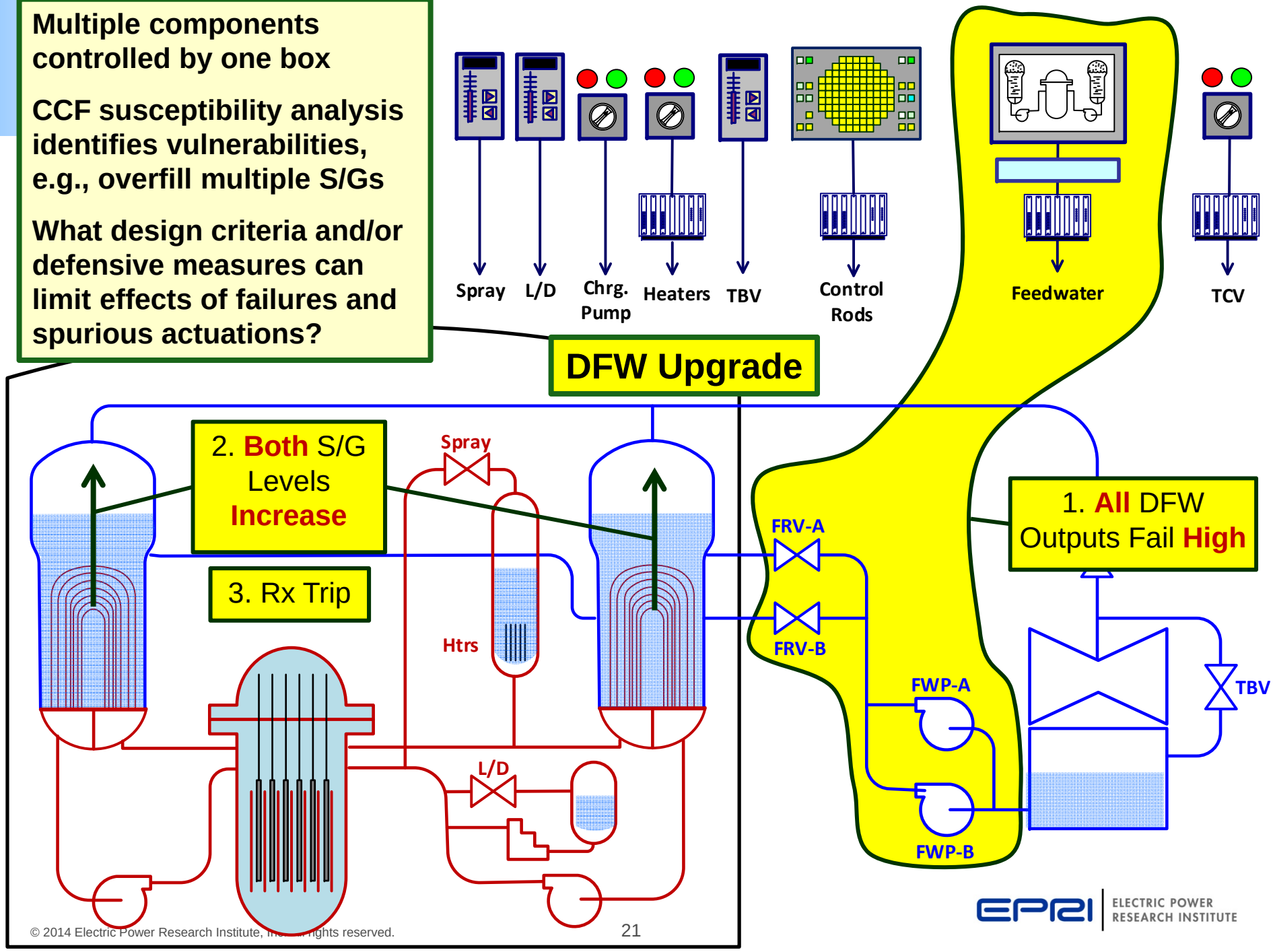


EPRI ELECTRIC POWER RESEARCH INSTITUTE

Multiple components controlled by one box

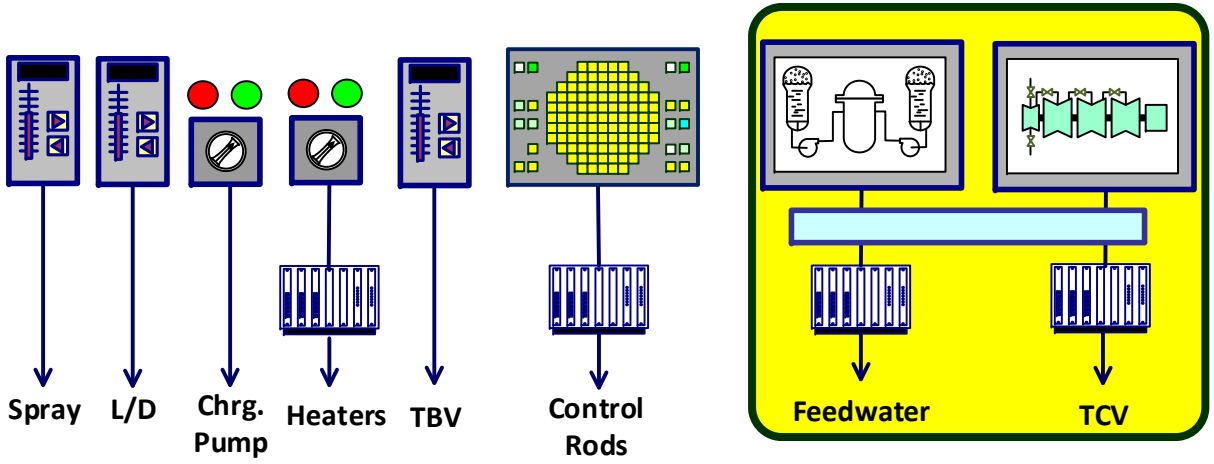
CCF susceptibility analysis identifies vulnerabilities, e.g., overfill multiple S/Gs

What design criteria and/or defensive measures can limit effects of failures and spurious actuations?

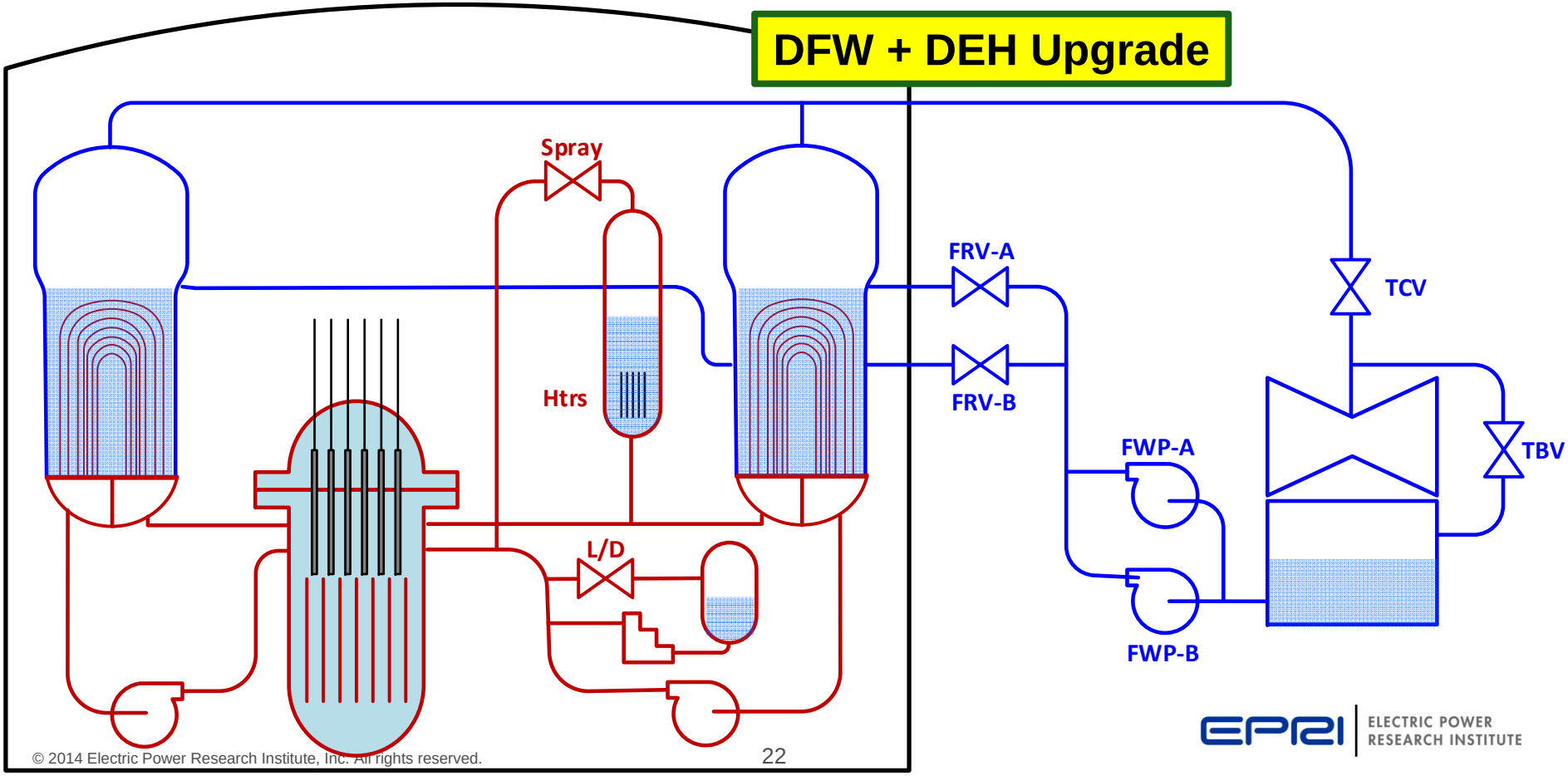


EPRI ELECTRIC POWER RESEARCH INSTITUTE

Now add a turbine control segment to the DCS architecture



DFW + DEH Upgrade

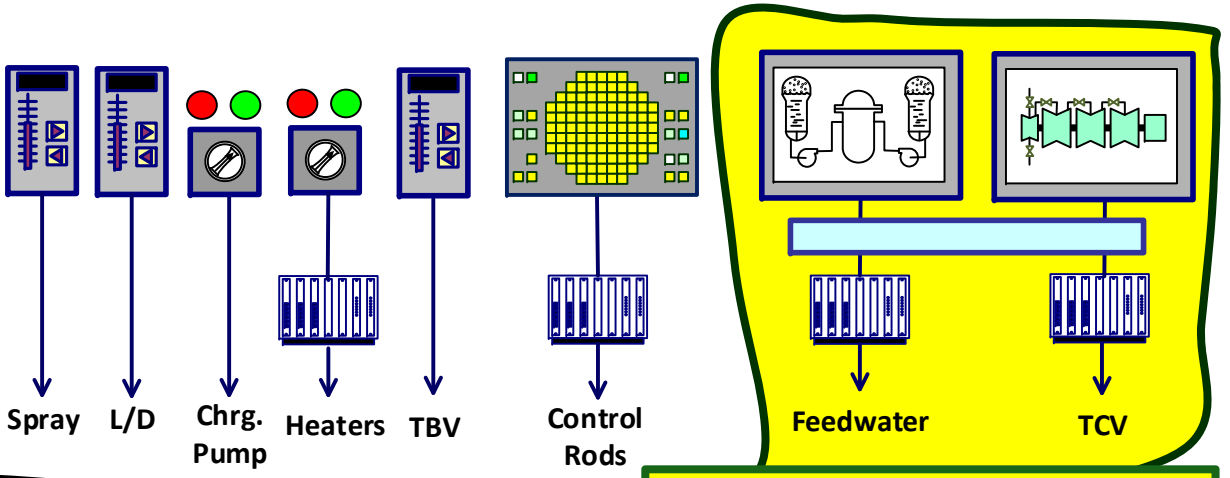


ELECTRIC POWER RESEARCH INSTITUTE

Segmentation, functional separation **reduce the failure effects**

What coupling mechanisms remain (power supply, HSI, communications, etc.)?

What failures & undesired behaviors are still plausible? Why?

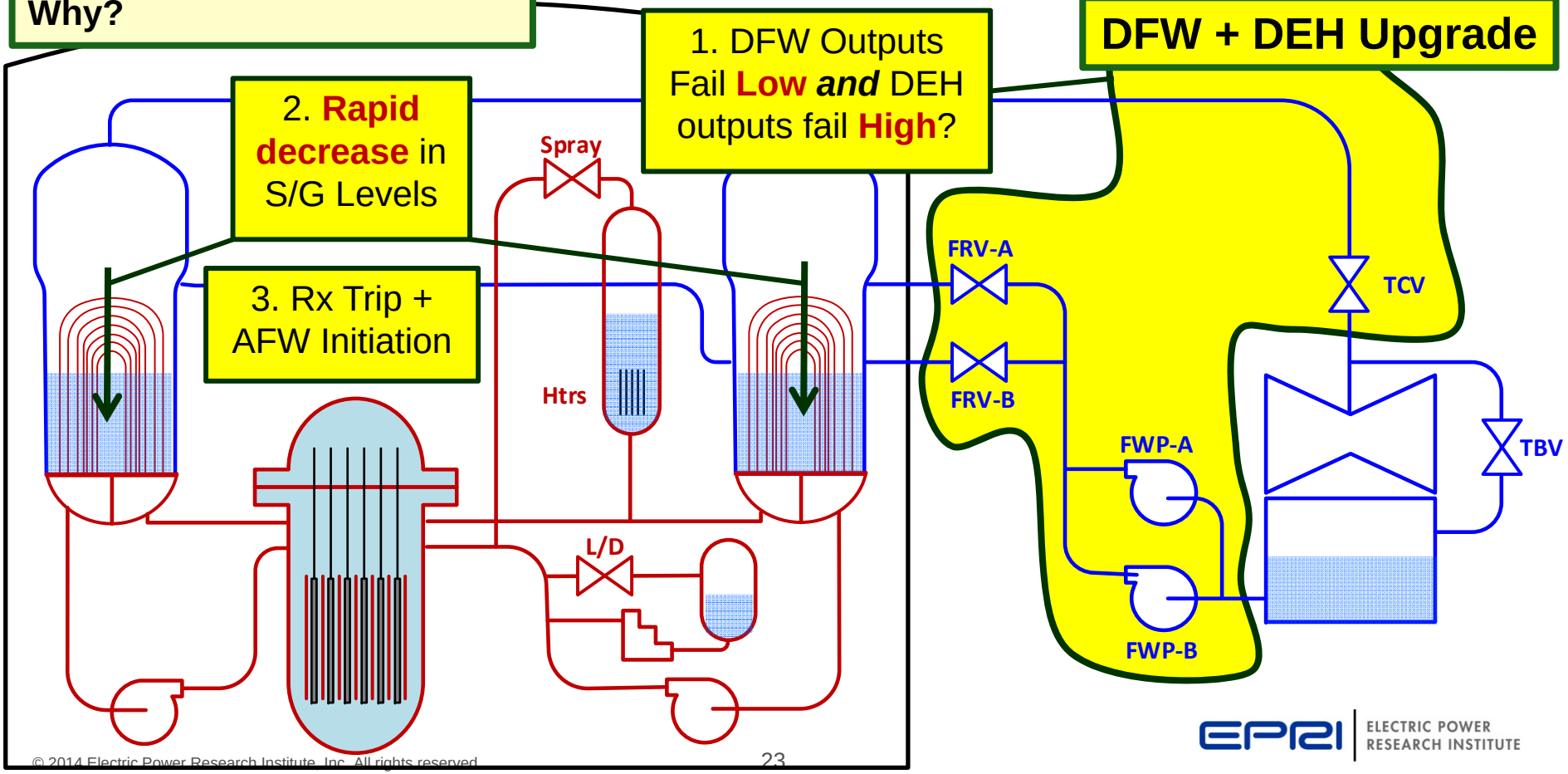


DFW + DEH Upgrade

1. DFW Outputs Fail **Low** ***and*** DEH outputs fail **High**?

2. **Rapid decrease** in S/G Levels

3. Rx Trip + AFW Initiation



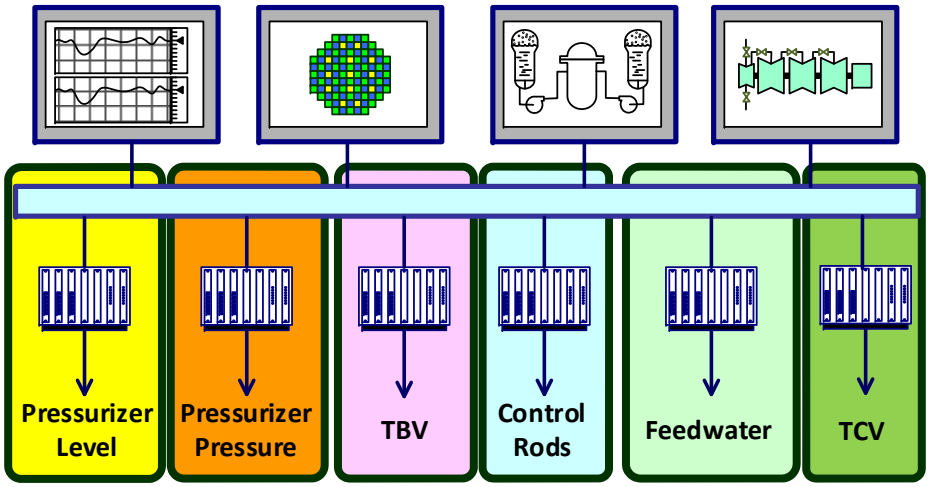
EPRI ELECTRIC POWER RESEARCH INSTITUTE

Now add more control functions using same communications, HSI, and software

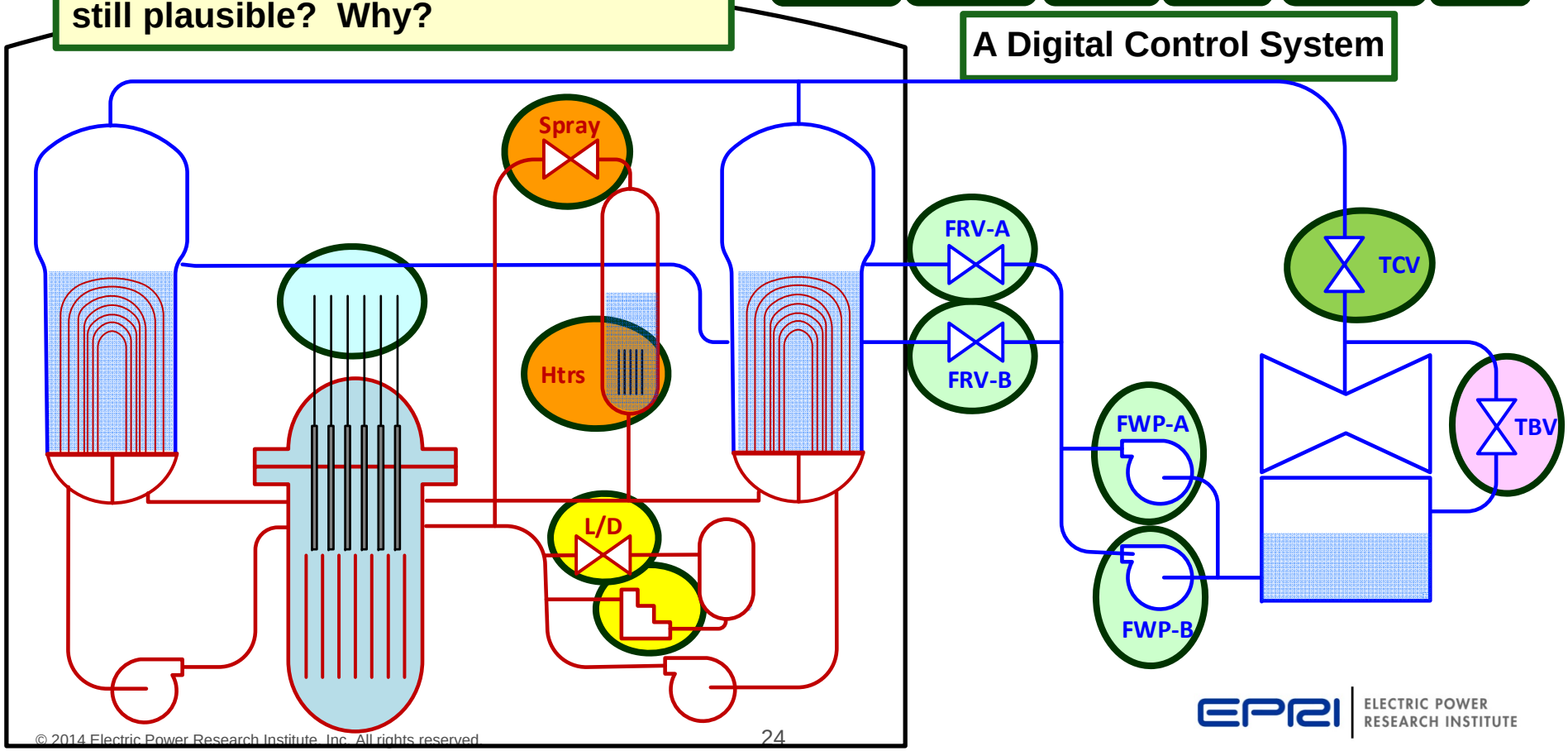
Failures and misbehaviors could affect single or multiple segments

Design measures, including ***segmentation***, help protect against CCF

What failures/undesired behaviors are still plausible? Why?



A Digital Control System



EPRI | ELECTRIC POWER RESEARCH INSTITUTE

Together…Shaping the Future of Electricity