LAWRENCE LIVERMORE LABORATORY

6

November 16, 1981

Frank D. Coffman, Section Leader
Systems Interaction Section
Reliability and Risk Assessment Branch
Division of Safety Technology, NRR
Nuclear Regulatory Commission
Washington, D.C. 20555

Dear Frank:

As you requested, we have reviewed the October 1, 1981 draft of Chapters 5 and 6 of the Initial Guidance for the Performance of Systems Interaction Reviews at Selected LWR's. Our comments have been incorporated into the enclosed revised draft of Chapters 5 and 6. Our recommended alterations appear directly in the text and are delineated by vertical lines.

Our most significant areas of disagreement with the earlier draft include:

1. Our concern that if an explicit analytic evaluation procedure is not used, the voluminous identified systems interactions all become negotiable. They must, therefore, be fixed or ignored on a case-by-case review between NRC and the utility.

2. The choice of explicit analytic evaluation procedure significantly affects the choice of identification procedure. In order to evaluate systems interactions in terms of their consequence, for example, the identification procedure must provide compatible output.

3. Training simulators are not faithful replicas of power plants and could give misleading results. Nevertheless, if they were used, they would require many thousands of simulator experiments. The identified systems interactions would not all be capable of being evaluated through the end-result of the experiment.

4. Results of the current IREP program are now becoming available and lessons learned from this effort should be reflected in the systems interaction program.

I look forward to hearing your comments on these proposed revisions.

Sincerely,

H.P. Alesso

RHVG
1/19/81 7
Ray Gallucci, PNL
NUREG/CR-1896

BCL-PNL REPORT SUMMARY

- system is collection of components which perform some function - the function defines the system *

- interaction occurs when conditions in one system affect (degrade) the ability of another system to perform its function *

- operator considered as a component *

- failure criterion must recognize potential as well as actual risk from an SI

- safety function = group of actions that maintain the defense-in-depth concept and minimize the potential of radioactivity release to the environment

  - 10 safety functions:

    1. reactor control
    2. reactor coolant system inventory control
    3. reactor coolant system pressure control
    4. core heat removal
    5. reactor coolant system heat removal
    6. containment isolation
    7. containment temperature & pressure control
    8. combustible gas control
    9. maintenance of vital auxiliaries
    10. indirect radioactivity release control

  - SI = system failure combinations that can reduce the effectiveness of any one of a # of basic safety functions

  - potential for SIs results from complexity of plant (use of redundant systems & components)...in their absence, single failures would dominate plant reliability *

  - methodology must be:

    1. systematic → (repeatable, thorough, unambiguous)
    2. complete
    3. flexible
    4. reproducible
    5. simple
    6. visible

    - also, must identify & evaluate SIs

- screening SIs:

  1. probability - however, does not reduce extent of detailed analysis
  2. safety function importance
  3. immediacy of required action (time dependence)
  4. categorical

  - screening should be done at early phase to reduce potential # of SIs needed for analysis

- SIs occur either on system or component level sequentially or coincidentally

- identificative methodologies:

  - system level:

    1. operational survey
    2. system FMEA

  - component level:

    1. operational survey
    2. physical survey
    3. component FMEA
    4. diagraphs

- evaluative methodologies:

  - full hierarchy (functions, systems, components):

    1. cause-consequence (event tree/conditional fault tree)
    2. consequence fault trees
    3. GO

  - partial hierarchy:

    1. Markov (system & component)
    2. weighting factors (component)
    3. Marshall-Olkin (component)
    4. generic analysis (component)

  - time:

    1. GO
    2. Markov
    3. phased mission

  - logic models appear to be most promising SI identification techniques.

  - focusing immediately upon commonalities couplings among components leads to an overwhelming # of potential candidates

- focus on basic safety functions & adopt logic models to evaluate system behavior on a system level

- event trees most appropriate at system level

- consequence fault trees can be used for evaluation of SIs (resolution limited to subsystems & major components)

- human errors:

  - dynamic (action during operation)

  - latent (calibration, testing, etc.)

- there are advantages to using same methodology for qualitative & quantitative analyses:

  1. facilitate consistent transition
  2. permit whatever degree of iteration is required
  3. flexibility provided for level of resolution
  4. enhanced visibility

- interim SI methodology

  1. simplified systems analysis

     - for each safety function in each plant mode

       i. determine system success paths, including major subsystems & components
       ii. determine vital auxiliaries
       iii. identify

          1. single failures disabling 2 systems
          2. common subsystems & components
          3. different subsystems & components linked by commonalities

COUPLING
1. only way coupling exists is if a 1. concurrence...
2. only way 2 can occur is if the common components of the subsystems form the coupling.
3. commonalities = coupling

  2. review of procedures, tech specs, & training requirements

     - more of a preventive method for human error

     - reviewer should check for violation of such requirements

  3. plant walk-thru

     - supplement earlier operational survey (inspectors provided with detailed drawings on "where to look")

BNL REPORT SUMMARY

- SI = existence of two dependent failures A & B such that $P(AB) \neq P(A) \cdot P(B)$
- SI = common-mode failure
- SI importance based on risk
  - SI risk compared to that from WASH-1400
- Initial SI focus on core melt...also, include containment breach modes
- Supplement risk quantification method with set of heuristic rules of good design practice (easier to identify than accident scenarios)

  rules that stimulate and guide further investigation

  - Such rules can be ascertained from "near miss" accidents & accident sequences developed by analysts

    1. Human Error
    2. Component Alarms
    3. Limit Frequency of Accident Initiators (Small LOCAS & Loss of Offsite Power)
    4. Physical Separation for Redundant Trains (cable fires)

  - Accident sequences may be overlooked by analyst, but keying on the violation of rules of good design practice can compensate for this
- SI methodology applied to ALL plant modes
- Consider all initiating events (entire spectrum of LOCAs & transients)
- Consider test & maintenance
- FMEA: recommended by ACRS to find SI within an interconnected electrical or mechanical complex
  - CMFA = common-mode failure analysis
  - CFA (cascade failure analysis) - systematic application of FMEA to find effects on other systems
  - include potential spatial commonalities (common environments)

- Walk-thru: plant specific

  - interactions among non-connected systems

  - Diablo Canyon seismic review

    - "Detrimental (systems) interactions are those that could conceivably compromise the function of safety equipment"

    - safety-related systems (& structures & components) = target
      nonsafety-related systems (& structures & components) = sources
      SI occurs if source affects a target

    - emphasis on spatial interactions among sources & targets

- Fault Trees (Sandia):

  - SI = "a situation where the likelihood of the undesired event is increased due to the relationship between two or more components"

  - SI is characterized by

    2. 1. mechanism ⟶ SI identification
    3. 2. probability } SI evaluation
    1. 3. consequence }

✓

- Interactions between components that affect the probability of failure of critical sets of components may be classified as:

  1. Connections (physical/spatial links between components)
  2. Functional Interdependences (state dependences) among components
  3. Human Error

    - Connections

      - physical connection as a common-cause source derives from syndrome of "perfect switch" (as reliability of components increased, that of the switch began to dominate failures) evolution of reliability

      - links are no more than "components" gates on fault trees ?

    - Functional Interdependences

      - change in state of one component affects probability of another in changing its state (usually due to environmental changes)

      - improper input from a component prevents another from performing its function (applicable for components with multiple failure states)

- Human Error
  - SI due to human error is possible when humans interact with more than 1 component of a system (normal operation, test, maintenance, etc.)
  - not handled by fault trees
- No one methodology can overcome problem of hidden commonalities
- Event/Fault Trees
  - TOPS are system fault trees (conditional)
  - event + fault trees reduces complexity of fault trees alone
  - FMEAs & Walk-thrus best used to assist event & fault trees
- Discussion of Systems Interaction Events that have occurred
  - See Table 1

TABLE 1. Would Methodology Identify Incident?

Incident	FMEA	Walk-Thru	Fault	Event/Fault	Practices Violated
BF3 Partial Scram Failure	Possibly	No	No	No	Need for Alarms (on SDV)
BF1 Fire	No	Crawl-thru Yes	No	No	Physical Separation of Redundant Cables Human Error
Beznau 1 Pressurizer Relief Valve Failure	No	No	No	Yes	Potential for Human Error (Operator Action Needed to Prevent Serious Accident)
TMI 2 Small LOCA	No	No	No	Yes	Human Error Need for Alarm (Relief Valve Position)
Davis Bessel loss of RHR (during refuel)	Possibly	No	No	No	Failure to Recognize Alternative System Arrangement during Non-Power Mode
Zion 2 DG Fire	No	No	No	No	Failure to Consider Plant Mode other than Power OP Human Error

- Combination of methods needed to identify various SIs

Cause ⟶ Effect	Effect ⟶ Cause
FMEA	Fault Tree
inductive reasoning	deductive reasoning

- Quantitative evaluation of importance of SI is best accomplished by event/fault trees (using info. from FMEA & walk thru)

  - Screen on risk

- Regarding past SI events, one should examine what else could have happened & obtain estimates of probability & consequence

- Risk-oriented evaluation suffers from the possibility of aggregated risk contribution from overlooked accident sequences being nonnegligible... therefore, as a supplement, search for violations of "good design practice" rules

LLL REPORT SUMMARY

- SI is concerned with the degradation of safety functions as well as total failure

    - inclusion of degradation is important

degree of degradation is such that the safety function could be lost by one additional failure

- non-safety reactor components & systems must be considered
- the kind of failures identified in conventional reactor safety analyses should be excluded from an SI analysis
- SI is a sequence of events such that the following are involved:

    1. the degradation of a reactor safety function
    2. two or more reactor systems, at least one of which is a safety system
    3. more than random failures & their expected consequences

- hierarchy of reactor safety functions:

    1. fundamental → defined by the undesirable outcomes they are designed to prevent
    2. general → must be performed to ensure safe operation & shutdown, regardless of plant mode or condition
    3. conditional → result from general safety functions when sub-divided according to plant conditions

SI Reviews look for conditions that lead to the conditional safety functions.

- Fundamental:

    1. reactor core protection
    2. mitigation of consequences of core-related accidents

- General:

    1. reactor subscriticality (RS)
    2. heat removal (HR)
    3. containment integrity (CI)

- Conditional: based upon conditions of "NO LOCA" (corresponding to ANS/N-18 conditions I & II) & "LOCA" (ANS/N-18 III & IV)

    1. reactor subcriticality

        i. reactor trip (LOCA or no LOCA) [RT]

    2. heat removal

        i. No LOCA

            - reactor coolant pressure boundary (RCPB)
            - reactor coolant recirculation (RCR)

ii. LOCA

- reactor coolant injection (RCI)

- reactor coolant recirculation (RCR)

3. containment integrity (LOCA only)

   i. post accident heat removal (PAHR)
   ii. post accident radiation removal (PARR)
   iii. containment isolation (ISO)

- LOCA: RT, RCI, RCR, PAHR, PARR, ISO
- No LOCA: RT, RCPB, RCR

- systems are associated with each general & each conditional safety function

- general safety systems:

  1. RS ⟶ reactor control system
  2. HR ⟶ reactor coolant system & connected systems
     emergency core cooling system
  3. CI ⟶ engineered safety features & containment systems

- ideally, associate SIs with conditional safety systems...however, revert to general safety systems when info. is lacking

- reactor systems divided into frontline & support systems, the frontline being further divided into normal operation systems & engineered safety features
  + accident

- SI classes:

  1. common mode failures propagated through reactor support systems
  2. common mode failures due to shared locations that are not propagated through reactor or support systems
  3. latent human errors & inherent problems
  4. dynamic human errors
  5. failures that result from reactor degradation

- event sequence categories:

  1. initiating events

     i. internal - associated with normal reactor operation
     ii. external - involve energy sources not associated with normal reactor operation

  2. human interfaces

     i. latent human errors - human actions that occur before an accident sequence that causes a degradation that is not obvious until the system is needed
     ii. dynamic human errors - actions, usually by the reactor operator, that exacerbate a reactor sequence

3. resulting reactor events

   i. expected or normal sequences - reactor performs as designed and as expected in response to an initiating event
   ii. common mode failures - multiple component failures traced to a common event
   iii. associated events - degradation of 1 system in a reactor sequence increases failure likelihood of another in a more complicated or more subtle way than a common mode failure

- random failure causing a normal resulting reactor sequence is NOT an SI

- SI evaluation methodologies: (See Tables 2 & 3)

1. analytical

   i. graph-based analysis
   ii. analysis-by-parts
   iii. on-line decision aids

2. non-analytical

   i. reviews of reactor operating experience
   ii. on-site inspexions

- diversion path analysis - safeguards analysis technique that searches for a specific, credible, unfavorable scenario

  - SI application: (See Table 4)

    1. associate descriptive attributes that indicate relative likelihood of occurrence with each SI scenario
    2. rank likelihood of each scenario
    3. assign "prevention strategy" to each scenario
    4. assess likelihood of scenario leading to SI
    5. assign score to each prevention strategy based on scenario feasibility & potential problem
    6. sort out results to identify SI weaknesses

- gross hazards analyziz - FMEA that assesses failure modes for systems rather than components

TABLE 2

Methodology	Type of SI Identified
reviews of reactor operating experience	no particular focus good, because an overview is needed
analysis-by-parts	local effects or gross sequential effects on a system caused by component or subsystem failures automatic response
graph-based analyses	shared support systems - dependencies hierarchies through pipes & wires
on-site inspections	shared locations & inherent relations
on-line decision aids	minimize dynamic human errors, usually through instrument & control systems

TABLE 3

Methodology	Examples	Strengths	Weaknesses
• reviews of reactor operating experience	• LERs • special studies	• identify problems "assumed away" in design	• cannot capture low frequency events
• analysis-by-parts	• FMEA • diversion paths analysis	• simple to perform & require analyst to systematically review for failures	• depend entirely on analyst's creativity & capture only local effects
• graph-based analysis	• fault trees • event trees • logic diagrams • influence diagrams	• exhaustive within boundary conditions • systematically cover low-frequency events	• analyst-dependent • limited in identifying latent human errors
• on-site inspections	• QA programs • walk-thrus	• focus on human problems & incorporate expert opinion under no formal constraint	• treat only static conditions & depend upon judgment of
• on-line decision aids	• automated displays • data retrieval systems • computerized status analysis • option generation systems	• reduce human dynamic errors	

TABLE 4

Methodology	SI class for which most pertinent
• reviews of reactor operating experience	• common mode failures propogated thru support systems • common mode failures propogated outside of reactor & support systems latent human errors & inherent problems
• graph-based analysis	• common mode failures propagated through systems • common mode failures propogated outside of reactor & support systems
• on-site inspex	• common mode failures propogated outside of reactor & support systems • latent human errors
• on-line decision aids	• dynamic human errors
• analysis-by-parts	• supplemental to above 4 methodologies

CONSENSUS

- Definition of SI: 3 important concepts

  1. degradation of safety function
  2. dependence
  3. at least two systems involved

- An SI is that resulting from dependencies between two or more systems which degrades a safety function.

Safety Functions

Conditional (based on ANS/N-18)

General	No LOCA (ANS/N-18 Conditions I & II)	LOCA (ANS/N-18 Conditions III & IV)
• Reactor Subcriticality →	→	→
• Core Heat Removal	• Reactor Coolant Pressure Control	X
	• Reactor Coolant Inventory Control →	→
	• Reactor Coolant Recirculation →	→
• Containment Integrity	X	• Containment Isolation • Containment Temperature Pressure Control • Combustible Gas Control • Radiation Removal

- Classes of SIs:

  1. preclusive system failure, i.e., failure of one system prevents another from operating, although available.

     e.g. → during a small LOCA, failure of the automatic pressure relief system, given prior failure of the high pressure coolant injection system, prevents operation of any of the low pressure emergency core cooling systems due to too high a reactor vessel pressure.

2. failure of a single component or dependent failure of more than one component common to two or more systems

   e.g. ⟶ failure of the LPCI/RHR pumps, common to both the low pressure coolant injection and the residual heat removal systems, fails both these systems.

3. failure of a support system common to two or more systems

   e.g. ⟶ failure of AC electric power, vital to several plant systems

4. dependent failure of different components in two or more systems

   e.g. ⟶ operator erroneously shuts off the control rod drive and the high pressure coolant injection pumps as sources of reactor vessel makeup water.

- Dependent failure causes:

  1. Human Error

     i.. dynamic - operator action/inaction
     ii. latent - "residual" error, such as one during testing, calibration, or maintenance, left undiscovered

  2. Spatial Commonality

  3. Functional Interdependence

     i. state dependence - change in state of one component affects another's probability of changing its own state (often due to environmental change)
     ii. improper input from a component prevents another from performing its function (applicable to components with multiple failure states)

- Methodologies for SI Analysis:

  1. Non-Analytic

     i. General

        1. LER review
        2. review of other sources of industry operating experience

     ii. Plant-Specific

        1. review of plant's operating history
        2. review of plant's tech specs
        3. review of plant's QA program
        4. walk-thru
        5. search for violation of rules of "good design practice"

2. Analytic

   i. Comprehensive

      1. fault trees
      2. event trees (+ conditional fault trees)
      3. influence diagrams

   ii. Supplementary

      1. FMEA (both system & component levels)
      2. common-cause generic analysis
      3. diversion path analysis
      4. digraph methods

- SI screening possibilities:

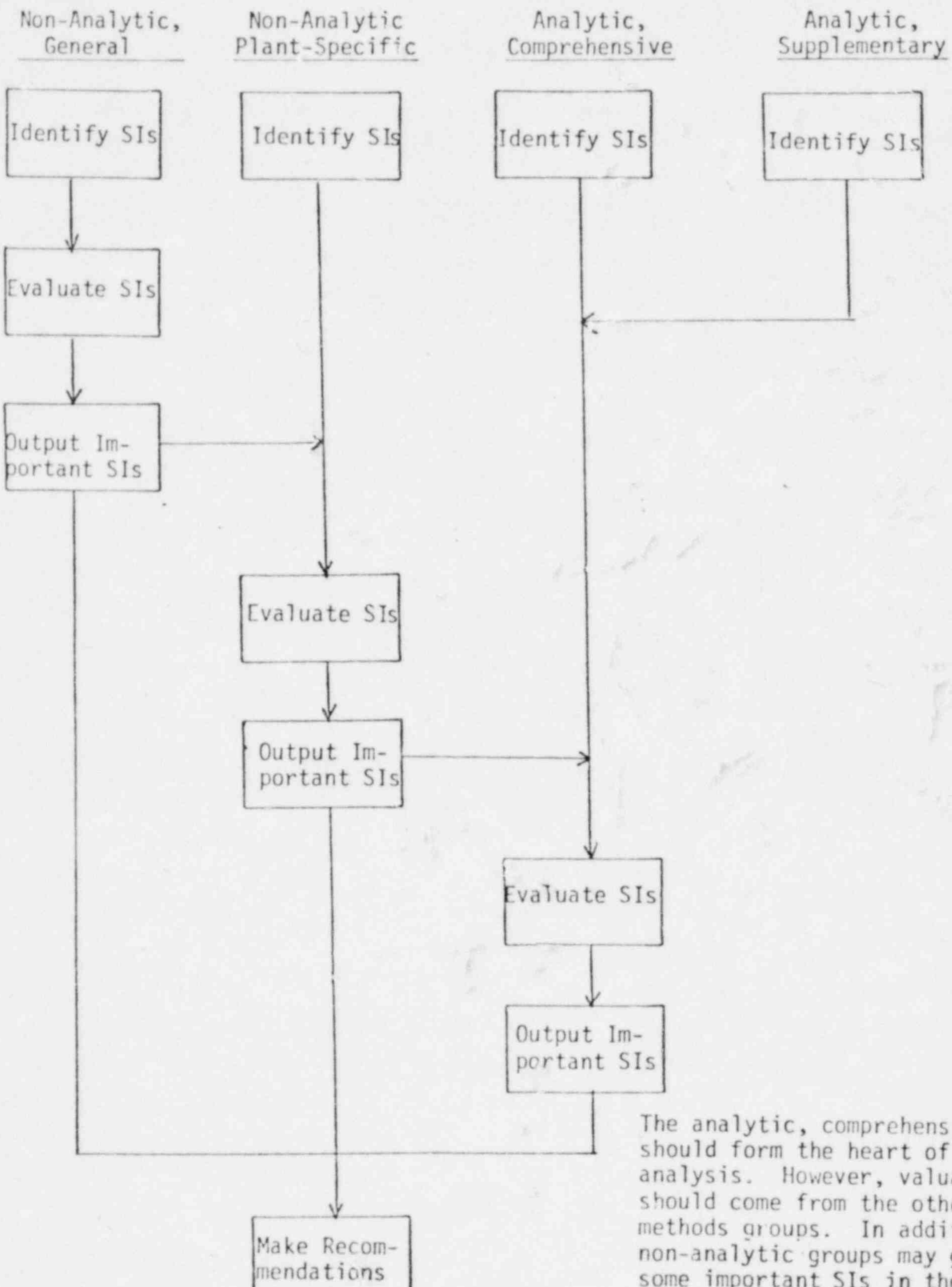
  1. risk
  2. probability
  3. immediacy of required action (time dependence)
  4. categorical
  5. importance
  6. weighting factors

TABLE 5

Methodology Category	Systematic	Simple	Complete	Reproducible	Flexible	Visible	Analyst-Independent	Identifies Human Error	Captures Low Frequency Events
Non-Analytic, General	No	Yes	No	Yes	Yes	Yes	Yes	Yes	No
Non-Analytic, Plant-Specific	No	Yes	No	Yes	Yes	Yes	No	Yes	No
Analytic, Comprehensive	Yes	No	Yes	Yes	No	Yes	No	No	Yes
Analytic, Supplementary	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes

TABLE 6

ROLES OF VARIOUS METHODOLOGIES IN SI ANALYSIS:



The analytic, comprehensive methods should form the heart of the SI analysis. However, valuable input should come from the other three methods groups. In addition, the non-analytic groups may generate some important SIs in their own right. Note that the prime role of the analytic, supplementary methods is, as the name implies, an auxilary one.

Contrast of SI Review and PR Assessment

FEATURE	SI REVIEW	PR ASSESSMENT
1. Failure Events Considered	• Random initiators* • Commonly caused events *Includes external initiators	• Randon initiators • Commonly caused events • Independently caused events
2. Ultimate Criterion	Degradation of systems independence	Unacceptable release of radioactive material
3. General Criteria	• Reactor Coolant Pressure Boundary shall be maintained • Those systems relied upon to transfer decay heat from reactor to ultimate heat sink shall be unimpaired. • Those systems relied upon to render and keep the entire core subcritical shall be unimpaired. • The Engineered Safety Features including those for the control of radioactivity shall be unimpaired.	Reduce** the risk from the most likely sequences **Numerical criteria are under development.
4. Probability Theory	• Not used to identify systems interactions • Probably used during ranking, although not necessarily.	• Used both to identify common cause events and to identify branches requiring no further resolution. • Used to analyze consequences
5. Objective	To identify, and rank by relative importance, those preconditions that degrade the general criteria as a consequence of an intersystems dependency.	To identify, and rank by relative importance, those accident sequences that contribute most to the unacceptable release of radioactive material as a consequence of all feasible combinations of dependent and independent failures.
6. Results	Fully characterized, mechanistic preconditions at a plant for engineering evaluation.	Consistent, risk basis for management decision on resource allocation.

I. Ideal features of a plant for the ability to conduct a Pilot SI Review

- Final stages of OL, i.e., both nearly complete and prior to fuel loading
- Control room Simulator available and similar to ref. plant
- Site specific hazard
- Program for Operational Reliability, e.g., IREP, PRA, feedback of operating experience
- Available resources
- Complexity in support systems, i.e., some of the SEP old plants may not be sufficiently complex.

II. Strategies for Selection of Pilot Review Plant

- Utility volunteers or negotiates for partial immunity to future requirements.

- Since H. Denton requires NTOL submittal and staff "concurrence," then threaten to not write off until utility commits to participate in pilot review on schedule.

- Since IREP inadequately covered externally initiated events, then require follow-on SI effort for externally initiated events and selected dependencies on more nonsafety-grade systems.

- Consider SI review as part of a site-specific hazard review.

III. Short Description of What the utility should do

o Objective of SI Review Process:

Perform a systematic evaluation for a condition where a failure of nonsafety-grade components, systems, or structures would violate four basic safety criteria. (4 criteria:

1. impairment of systems for decay heat removal

2. impairment of systems for primary coolant inventory

3. impairment of systems for entire-core shutdown

4. impairment of ESF and systems for radioactivity control)

These conditions are due to hidden connections within the design where past assumptions of independence (either stated or implicit) can be shown to be erroneous. The important regulatory impact is that such connections would demonstrate inaccuracies in past safety analyses prior to their occurrence during plant operations.

o Products of SI Review Process:

Fully characterized adverse systems interactions, i.e.,

1. criteria violated and degree of impairment

2. couplings (nature of physical connections)

3. Initiat~~ion~~ or or initiators

4. ~~ex~~ in ternal ~~automatic~~ scenario

5. external ~~mechanistic~~ scenario

6. hidden dependency (i.e., propagating features, CCF)

o Process of SI Review

1. Select important support systems by dependency grading.

2. Systematic identification of hidden connections to the selected systems (the "what if" step).

   a. ~~Internally initiated~~ Functionally coupled

   b. ~~Externally initiated~~ Spatially coupled

   c. Humanly coupled

3. Fix the SIs that yield functional consequences exceeding the present licensing basis (infers utility analysis).

4. Recommend modifications to interim guidance so that it could become a Regulatory Guide.

5. Document both their analysis of the plant and their recommenations on a Reg. Guide.

IV. Idea of Level of Effort

NRC

2 1/2 staff over 1 1/2 year

$450K T/A funds over 1 1/2 year

(3 labs at $150K each)

Utilities

Either o Each utility perform a total SI review of its plant at an estimated cost of each total program being upper bound for pilot $2,000K over 1 1/2 year.

or o "n" utilities perform $1/n^{th}$ of a total SI review of its plant, e.g., 2 utilities each over 1 1/2 year doing 1/2 of a total SI review. Total program divided by type of SI initiator. (costs appear uniformly distributed by type of SI). may not save much by dividing up

or o 3 utilities perform selected samples of a total SI review. Total program divided by type of SI initiator with emphasis on Internally initiated SIs.