27
4-12-82
JMB
10 w/ NTIS

①

LR. 413

I-2502

UCID- 19130

MASTER

REVIEW OF THE PASNY
SYSTEMS INTERACTION STUDY

H. P. Alesso
Lawrence Livermore National Laboratory

UCID--19130

DE82 012527

March 1, 1982

Lawrence
Livermore
Laboratory

This is an informal report intended primarily for internal or limited external distribution. The opinions and conclusions stated are those of the author and may or may not be those of the Laboratory.

This work was supported by the United States Nuclear Regulatory Commission under a Memorandum of Understanding with the United States Department of Energy.

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

This document contains information that is the property of the United States Government. It is loaned to you for your use only. It is not to be distributed outside your organization. It is not to be used for any purpose other than that for which it was loaned to you. It is not to be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or by any information storage and retrieval system, without the prior written permission of the United States Government. The United States Government is not responsible for any errors or omissions in this document. The United States Government is not responsible for any damage to property or persons resulting from the use of this document. The United States Government is not responsible for any loss of data or information resulting from the use of this document. The United States Government is not responsible for any other consequences resulting from the use of this document.

1.0 OBJECTIVE OF REVIEW

The objective of this review is to evaluate and make recommendations on the Systems Interaction (SI) methodology proposed by the Power Authority of the State of New York (PASNY) for application to Indian Point No. 3 (IP-3).¹

2.0 BACKGROUND AND MOTIVATION OF REVIEW

A systematic procedure for the identification and evaluation of systems interactions is being developed by the NRC. Contributions by Battelle Memorial Institute and Brookhaven National Laboratory are being used for the development of future guidance and regulations. In addition, the Lawrence Livermore National Laboratory (LLNL) is assisting NRC in reviewing PASNY's proposed methodology for application to IP-3. It is expected that experience and knowledge gained from the IP-3 application will lead to modifications of the SI efforts in other areas of the NRC program.

3.0 STATEMENT OF PROBLEM

This review must judge if PASNY's proposed SI methodology can succeed in solving the following problems:

1. identify SIs for nonconnected and interconnected systems for IP-3,
2. evaluate the associated safety hazard or risk of the SIs for nonconnected and interconnected systems for IP-3,
3. ensure that the NRC proposed scope² of the problem is covered, and
4. provide insight for others working toward NRC SI regulations.

4.0 OUR REVIEW APPROACH

Our preference for a SI identification and evaluation procedure for application to Indian Point-3 was presented in our LLNL reports.^{3,4} However, we have evaluated the PASNY proposal on the basis of its own merits to address the problems involved in SIs (see Section 3.0).

We examined the PASNY general methodology¹ presented in Vol. 1 and the PASNY AFW example¹ presented in Vol. 2 against our review criteria given in Section 3.0. We referred to the NRC Staff Letter Report² and to the LLNL SI Evaluation for application to IP-3 Procedure³ for guidance and comparison.

Our definition of a systems interaction was taken from References 2 and 3. Recall that a systems interaction is a sequence of events leading to the violation of at least one vital safety criterion as a result of two or more component failures that are caused by a dependent failure (common-mode or common cause).^{2,3} The four vital safety criteria² are:

1. the ability to achieve and maintain the entire core subcritical;
2. the ability to transfer decay heat from the reactor to the ultimate heat sink;
3. the ability to maintain reactor coolant pressure boundary; and
4. the ability to provide Engineered Safety Features.

5.0 OUR RESULTS

The general methodology presented in Vol. 1 consisted of a nonconnected SI procedure and an independent interconnected SI procedure.¹ Before we continue with an evaluation of these two procedures, we would like to comment on the appropriateness of this partitioning of the systems interaction problem.

While the partitioning can adequately address the SI problem in general, it leads to two serious drawbacks. First, the two independent methodologies result in two different evaluation criteria. The interconnected SI evaluation is based on a FMEA analysis relating to the single failure criteria,¹ while the nonconnected SI evaluation rests heavily on experienced engineering judgment.¹

Secondly, it seems probable that two independent methodologies used to partition a single problem will lead to an inefficient expenditure of resources and effort. It has been amply demonstrated in other proposed SI procedures that a single methodology can be exploited for both nonconnected and interconnected SIs.³⁻⁶

In this section, we will continue with our critique of the PASNY SI study under the following four headings: (1) the PASNY Nonconnected Procedures, (2) the PASNY Nonconnected AFW Example, (3) the PASNY Interconnected Procedure, and (4) the PASNY Interconnected AFW Example.

The PASNY Nonconnected Procedure - The nonconnected SI procedure examined common cause events (e.g., a fire) and found all sources (non-safety-grade components) that could threaten the safety function of a target (safety-grade component).

This is accomplished by a multidisciplinary team of experts conducting an on-site walk-through inspection. Such an inspection has already been demonstrated as being a valuable SI identification method.⁷

The PASNY Nonconnected AFW Example - The nonconnected portion of the AFW example presented in Vol. 2 was a satisfactory example. It demonstrated the capability of the nonconnected procedure; and we found the photographs, discussion sheets, and cross-indexing to be a good format.

The PASNY Interconnected Procedure - Interconnected systems were defined as those mechanical and electrical complexes which are process-coupled to one another physically via piping, instrumentation tubing or electrical wiring. Included in this definition is HVAC equipment which, although not physically connected, may be necessary to support the continuous safe operation of interconnected systems.

Step 1 was the selection of specific systems for evaluation and is accomplished by developing functional shutdown logic diagrams that describe the general functions necessary to prevent core damage. These logic diagrams are based upon system descriptions; instrumentation and control logic diagrams; and electrical schematic, block, and wiring diagrams. In addition, important information about system interfaces is obtained at the site by inspecting physical facilities and by meeting with plant personnel familiar with the design, operation, and maintenance of the system.

Having described the safety functions and the specific plant safety systems, the next substep is to identify the required responses, or safety actions, that must be accomplished in order to achieve a safety function. The sensed variables that cause or require the system response are identified. In cases where the system does not automatically respond, the operator action required to initiate the safety system is identified (e.g., starting a pump locally or from the control room). As the safety systems and their action are identified, they are arranged in functional order forming success paths, or operation sequences, leading to the required safety function. The arrangement of success paths becomes the Shutdown Logic Diagram (SLD) for the event.

To depict the level of redundancy in the plant design on the SLD, a sufficient number of independent parallel paths is developed for each safety function such that no single component failure can prevent the achievement of the required safety function.

The second step, the identification of dependencies or commonalities, is accomplished by further developing the functional system shutdown logics into subsystems more commonly referred to as auxiliary diagrams. The auxiliary diagrams provide the link between the functional system and support systems necessary to achieve a safety function.

After completion of the SLD for a postulated event, each safety system displayed on the SLD is analyzed to determine the specific support requirements necessary to produce its safety action. Examples of these support requirements are electric power, component cooling, or instrument air supply. The analyst refers to the SLD to determine every sequence in which a safety system is required, thereby ensuring all support requirements are identified. After identification of the support requirements, the plant systems that provide these support requirements are identified. These systems are the Auxiliary Safety Systems. A Safety System Auxiliary Diagram is then prepared on which the prime safety system and its auxiliary safety systems are displayed.

In developing the Safety System Auxiliary Diagram the analyst ensures that each support requirement is functionally redundant by developing design information about the plant sufficient to positively identify the auxiliaries essential for the required response of the safety system.

To complete the Safety System Auxiliary Diagram the analyst must review the Shutdown Logic Diagrams for all the postulated events to identify all safety sequences in which the subject auxiliary safety system appears.

After completion of the Shutdown Logic Diagrams for each postulated event and the Safety System Auxiliary Diagrams, the Auxiliary Safety System Commonality Diagram (ASSCD) for each Auxiliary Safety System is developed. This diagram indicates all the safety systems that a given Auxiliary Safety System supports. The ASSCD is developed mainly as an information diagram, rather than a primary design-review diagram. The ASSCD allows evaluation of the overall plant response to the operations of each Auxiliary Safety System.

The Shutdown Logic Diagrams (SLD), Safety System Auxiliary Diagrams (SSAD), and the Auxiliary Safety System Commonality Diagram (ASSCD) are basically devices employed for identifying the safety and support systems (including nonsafety systems) that are to be analyzed for interactions, and for correlating and combining the results of FMEAs on individual systems in order to understand and portray how interconnections, couplings and dependencies among all systems can propagate nonsafety system failure(s) into the safety system. This analysis describes the combinations of components which would result in the loss of any of the four basic functions: (1) reactor-subcriticality, (2) decay heat removal, (3) reactor coolant pressure boundary, or (4) containment integrity.

The third step, evaluation of the systems interactions through the determination of their relative importance to safety, is accomplished by using deterministic logic, failure modes and effects analyses.

The failure mode and effects analysis (FMEA) provides for the evaluation of partial success or failure, off-normal operation (e.g., reduced flow), inadvertent operation, and time dependence. From these FMEAs, performed with the fault tree as a backdrop, interconnected system interactions are to be identified and evaluated.

The PASNY interconnected SI procedure as outlined above would provide a satisfactory approach toward identifying the interconnectivity between safety and nonsafety systems. This could lead to a satisfactory identification of systems interactions. Table 1 outlines the way this could be accomplished directly. This method includes a logic diagram model and finding path-sets and cut-sets of the model.

Table 1
Conventional Success-Path Risk Analysis

- Step 1. A success-oriented logic diagram is constructed to model the system.
- Step 2. Connectivity between safety and nonsafety systems is identified.
- Step 3. A reachability computer code is used to find all path-sets of safe, successful system operation.
- Step 4. A Boolean reduction code is used to find all minimum path-sets.
- Step 5. A commonality analysis could be done at this point or, alternatively, added analysis could have been done in Step 2 if computer limitations can be avoided.
- Step 6. Use De Morgan's Law to find all minimum cut-sets.
- Step 7. Discriminate between minimum cut-sets of significant failure.
- Step 8. Use ranking computer code to evaluate qualitative information.
- Step 9. Utilize failure data to conduct probabilistic analysis for quantitative evaluation.

In the PASNY SI interconnected procedure, however, no attempt is to be made to find path-sets. The motivation for this is apparently the additional work that PASNY is performing in a Probabilistic Risk Assessment (PRA) for IP.S. By referring to the minimum cut-sets of the system fault trees completed in their PRA, PASNY hopes to "short-circuit" the steps we have outlined in Table 1, thereby jumping from Step 2 directly to Step 7.

In Alesso, we discuss the relationship between diagrams, path-sets and cut-sets, and state that a flawless fault tree analysis of a system can in certain ways be a subset of a success-oriented analysis carried out on the same system.⁴ In the PASNY interconnected procedure, it is proposed to use their minimum cut-sets of their PRA as a "backdrop" to identify when interconnectivity between safety and nonsafety systems results in a systems interaction. In other words, when a group of components can be traced back to a common cause/mode failure due to a single non-safety component, that group is compared to the PRA system fault tree's minimum cut-sets. If that group does not form a cut-set it can be considered as much less important than if it does.

It is highly debatable if the use of minimum cut-sets as a backdrop can be considered satisfactory. Ineoretically, the mathematical relationships could be valid. However, in practice this "short-circuit" is highly suspect. In addition, if the PRA systems fault tree covered the SI problem correctly down to this level of detail, why do a separate SI? Why not merely expand the PRA study to include the commonalities of nonsafety systems, shared environmental conditions and dynamic human error?

Next, we critique the PASNY interconnected evaluation procedure consisting of a FMEA review of a single component in light of a common cause event.

In general, a FMEA review by itself is inadequate in evaluating interconnected SIs. This is because it requires the analyst to make a subjective judgment that he is not qualified to make. He is asked to decide whether a combination of component failures (occurring due to a dependent failure) can lead to an undesirable consequence (like core damage) and how this SI ranks in relation to other SIs. The ranking is necessary in order to decide which repairs are to be given priority and which may be neglected.

The PASNY use of FMEA to evaluate a single component failure in relation to its compromising "its intendant safety function"¹ is inadequate. Single components (even ones conditional on events) are not systems interactions, especially when they do not "dig" into the non-safety grade support systems (such as non-safety control and instrumentation). It would be more appropriate to use FMEA, at this point, as a decision tool. FMEA could be used to decide if the safety grade component was dependent on a non-safety grade support system; then a qualitative analysis using a code like IMPORTANCE could be conducted, followed by a probabilistic quantitative analysis.

Another discrepancy in the SI interconnected procedure is the lack of sufficient consideration for dynamic human error as required in the scope of the SI problem.^{2,8}

The PASNY Interconnected AFW Example - The interconnected portion of the AFW example presented in Vol. 2 failed to demonstrate PASNY's interconnected SI procedure. This failure is a result of the following conditions:

1. It was inappropriate to select any single safety system for examination of the interconnected portion of the analysis and limit its boundary conditions, as in Vol. 2.
2. Auxiliary diagrams and commonality analysis were presented, but no demonstration of their capabilities was given.
3. No combination of component failures leading to an undesired consequence and resulting from a dependent failure were identified.
4. No connection was made between how the PRA fault tree and FMEA were used to evaluate SIs.

Table 2 summarizes our review conclusions. It gives a grade of satisfactory or unsatisfactory to various aspects of the two independent PASNY procedures for both the general methodology and the AFW example.

Table 2
Summary of Review Conclusions

	PASNY's general Methodology	PASNY's AFW Example
<u>Example For Nonconnected Systems Procedure:</u>		
1. Identifying SIs	SATISFACTORY	SATISFACTORY
2. Evaluating SIs	SATISFACTORY	SATISFACTORY
3. Covering NRC Scope	SATISFACTORY	SATISFACTORY
4. Usefulness to others	SATISFACTORY	SATISFACTORY
<u>For Interconnected Systems Procedure:</u>		
1. Identifying SIs	SATISFACTORY (?)	UNSATISFACTORY
2. Evaluating SIs	UNSATISFACTORY	UNSATISFACTORY
3. Covering NRC Scope	UNSATISFACTORY ^a	UNSATISFACTORY
4. Usefulness to others	SATISFACTORY	UNSATISFACTORY

^aDid not include dynamic human error SIs.

6.0 RECOMMENDATIONS

We recommend that:

1. PASNY continue to use their nonconnected SI procedure for application to all safety systems at IP-3;
2. PASNY further develop its interconnected SI procedure for identifying and evaluating SIs, document it in more detail, and provide a realistic demonstration of its capabilities. It should capture combinations of components whose failures are due to a dependent failure and which lead to a known consequence;
3. PASNY include dynamic human error in their interconnected SI procedure;
4. after a satisfactory interconnected SI procedure example has been reviewed by NRC and LLNL, PASNY should apply it to IP-3; and
5. others working in related NRC SI projects review the PASNY "Systems Interaction Study" for their own edification along with NRC's review of the study.

REFERENCES

1. Power Authority of the State of New York, Indian Point No. 3 Systems Interaction Study, Vols. 1 and 2, EBASCO Services, Inc. (January 1982).
2. U. S. Nuclear Regulatory Commission, "The Systems Interaction Branch Approach to Systems Interactions in LWRs," U. S. Nuclear Regulatory Commission, Washington, DC, Staff Summary Letter Report Draft (February 1981).
3. J. Lim, H. P. Alesso, T. R. Rice, R. K. McCord, and J. E. Kelly, Systems Interaction Evaluation Procedure for Application to Indian Point-3, Lawrence Livermore National Laboratory, Livermore, CA, NUREG/CR-2050 Draft (April 1981).
4. H. P. Alesso, Some Fundamental Aspects of Fault Tree and Digraph-Matrix Relationships for A Systems Interaction Evaluation Procedure, Lawrence Livermore National Laboratory, Livermore, CA, UCID Draft (March 1982).
5. A. Buslik, I. Papazoglou, and R. Bari, Review and Evaluation of Systems Interaction Methods, Brookhaven National Laboratory, Upton, NY, NRC Report NUREG/CR-1901 (January 1981).
6. P. Cybulskis, et al., Review of Systems Interaction Methodologies, Battelle Memorial Institute, Columbus, OH, NRC Report NUREG/CR-1896 (January 1981).
7. Pacific Gas & Electric Co., "Description of the Systems Interaction Program for Seismically-Induced Events, Diablo Canyon Units 1 and 2, Revision 2," Dockets 50-275/323, Pacific Gas & Electric Co., San Francisco, CA (July 9, 1980).
8. J. H. Conran, "Meeting Summary and Status Report," Dockets 50-247/286, Pacific Gas & Electric Co., San Francisco, CA (October 20, 1981).