NOTICE

**CERTAIN DATA
CONTAINED IN THIS
DOCUMENT MAY BE
DIFFICULT TO READ
IN MICROFICHE
PRODUCTS.**

Los Alamos National Laboratory is operated by the University of California for the United States Department of Energy under contract W-7405-ENG-36

TITLE IDENTIFICATION OF HUMAN ERRORS OF COMMISSION USING SNEAK ANALYSIS

AUTHOR(S) H. A. Hahn, J. A. DeVries

SUBMITTED TO Human Factors Soc.,
Sept. 2-6, 1991

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

By acceptance of this article, the publisher recognizes that the U.S. Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or to allow others to do so, for U.S. Government purposes.

The Los Alamos National Laboratory requests that the publisher identify this article as work performed under the auspices of the U.S. Department of Energy.

Los Alamos National Laboratory
Los Alamos, New Mexico 87545

Identification of Human Errors of Commission Using Sneak Analysis

**Heidi Ann Hahn and John A. deVries II
Los Alamos National Laboratory
Los Alamos, New Mexico**

Sneak Analysis was adapted for use in identifying human errors of commission. Flow diagrams were developed to guide the analyst through a series of questions aimed at locating sneak paths, sneak indications, sneak labels, and sneak timing. An illustration of the application of this methodology in a nuclear environment is given and a computerized tool to support Sneak Analysis is described.

INTRODUCTION

Within the field of probabilistic risk assessment (PRA), a great deal of emphasis has been placed on modeling hardware or machine contributors to system risks. Likewise, human reliability assessment (HRA) practitioners have followed a PRA mindset -- the human influence on risk has largely been categorized as if the human were a machine component that would either perform an action or not. That is, the PRA event tree will note that the operator failed to open a valve, failed to detect an alarm, and the like. These types of errors are fairly easy to identify; for any action expected of a human operator, there is the possibility of failure to comply. This approach, however, may result in the under-representation of human contributions to system failure, as it may omit "errors of commission" from the analysis.

Commission errors are incorrect or unplanned-for actions taken by an operator that serve as precursors for initiating events. Generally these are either errors in the execution of a task, in which the operator acts incorrectly or at an inappropriate time, or errors of intention, which are due to errors in problem solving or decision making.

This type of error has been largely unexplored as a contributor to risk, in part, because of the difficulty in identifying potential sources of commission errors. Sneak Analysis can be used for this purpose, and is especially powerful as an aid to discovering latent errors (Reason, 1990), those system defects which result from poor design, faulty maintenance, and/or poor management control and which increase the incidence of operator error.

SNEAK ANALYSIS

Sneak Circuit Analysis (Clardy, 1980) is a method for identifying a latent path in an electrical circuit that causes an unwanted event to occur or that inhibits a wanted event. Topological criteria allow recognition of the unplanned operational modes of the system.

Sneak Analysis Methodology

The following paragraphs briefly define the major steps involved in Sneak Circuit Analysis. Steps related to computer coding of data have been omitted, because they are not pertinent to the discussion of applying sneak analysis to human error which follows.

Data acquisition and encoding. In using Sneak Circuit Analysis, the first major consideration is to ensure that the data being used adequately represent the true system. In electrical systems, a detailed circuit schematic is needed to gain a full appreciation of hidden continuities and functional dependencies.

Encoding involves partitioning the data at key points. Encoding rules are used to ensure that the accuracy of the representation is maintained, while the data are simplified to eliminate non active elements.

Network tree production. Network trees represent a simplified version of the system, in that they selectively delete extraneous detail while leaving intact all elements pertinent to the understanding of system operation. In Sneak Circuit Analysis, network trees are characterized by their topological orientation. That is, all power sources are located at the top of the tree, while all grounds appear at the bottom of the tree.

Topological pattern recognition. Once a network tree has been produced, the analyst looks for topological patterns. As shown in Figure 1, these include the: (1) single line; (2) ground dome; (3) power dome; (4) combined dome; and (5) "H" pattern. One, or a combination of these patterns, will characterize the circuitry of a network tree. The analyst determines which patterns apply at each node of the tree, then identifies clues associated with the particular pattern to identify sneak circuit conditions. If all nodes are examined in this way, all possible sneak circuits will be identified.

Clue application. For each topological pattern, there is an extensive list of clues which help the analyst identify sneak circuit conditions. (There are more than 100 clues for the "H" pattern.)

These clues, in turn, lead to the identification of specific sneak conditions. Four major sneak conditions have been identified for Sneak Circuit Analyses. A **sneak path** occurs when flow can travel along an unexpected path. A **sneak indication** is an incorrect or ambiguous display output which may result in inappropriate operator action. Similarly, a **sneak label** on a control is one which is misleading and which may cause inappropriate actions to be taken by operators. **Sneak timing** causes functions either to occur when they are not expected or to not occur when they are expected.

Note that the same sneak circuit conditions can occur for more than one topological pattern. For example, both the combination dome and the "H" pattern have potential sneak paths. Applying all pertinent clues to each network tree for a system results in complete enumeration of all sneak circuits inherent in that system.

APPLYING SNEAK ANALYSIS TO HUMAN ERROR IDENTIFICATION

Clardy (1980) points out that Sneak Circuit Analysis should be applicable in other complex systems, as long as those systems are flow oriented. In many complex human-machine systems, operator actions are flow oriented, in that they result from following a step by step procedure. In such systems, Sneak Analysis methodology should be helpful in anticipating unplanned operator actions. The remainder of this paper is devoted to an illustration of the application of Sneak Analysis (using a computerized Sneak Analysis Tool) to the prediction of potential sources of human error in a nuclear power plant interfacing system loss of coolant accident (ISLOCA). Rather than relying on the identification of topological patterns, however, this application of Sneak Analysis methods uses a series of flow diagrams and checklists to guide the analyst in the identification of sneak conditions.

The Sneak Analysis Tool serves as an aid in performing Sneak Analysis. It poses a series of questions to the analyst, preserving the logic hierarchy of the Sneak Analysis flow diagrams

and terminating the search for a particular sneak condition when appropriate. It also serves as a report generator; at each point in the analysis, there is an opportunity to provide documentation of findings. This documentation can later be printed in various formats.

Data Description

The first step in performing Sneak Analysis or using the Sneak Analysis Tool is to provide a description of the system being analyzed. This description can either be text- or graphics-based.

As was the case with electrical systems, it is important for the analyst to be able to draw an accurate representation of the entire human-machine system, so that every step of the process can be subjected to analysis. For the purposes of this illustration, however, we will look at only one potential contributor to the ISLOCA, namely, the human-machine interaction in the decay heat removal (DHR) system. Figure 2 shows a flow diagram of the activities associated with the initiation of DHR. Figure 3 is a schematic representation of the letdown valves involved in DHR. Motor Operated Valves (MOV) DH-11/DH-12 are interlocked to the reactor containment system (RCS) pressure such that they cannot be opened if the RCS pressure is above 301 psi for DH-11 and 266 psi for DH-12. Of interest are the human errors of commission associated with the opening of valves DH-11/DH-12.

Clue Application

Next, Sneak Analysis guides the analyst through the clue application process. The analyst may choose the order in which sneak conditions are addressed. To give a flavor for how Sneak Analysis and the Tool work, we show a fairly detailed example of sneak indication analysis. In the interest of brevity, all other sneak conditions are simply represented by their logic diagram. The Sneak Analysis Tool represents all logic diagrams as a series of questions, similar to those provided for the sneak indication.

Sneak indication. The possibility of a sneak indication exists in a human-machine interface when the operator must obtain information from an output source. Figure 4 is the flow diagram which leads the analyst through questions needed to identify possible sneak indications. Note also that one node of the diagram indicates a sneak inhibit -- an error of omission resulting from failure of the operator to see or hear the indication, thus, fail to perform an indicated action.

Figure 5 shows how the Sneak Analysis Tool translates the flow diagram into a series of yes/no questions for the analyst to answer. In our example, a sneak indication would be possible if the operator needed to use input from an output source as an indicator to open valves DH-11/DH-12. Thus, the answer to the first question asked (i.e., Must the operator obtain information from an output source?) is affirmative. The schematic in Figure 2 shows that the operator is to open the valves after verifying that the RCS pressure has dropped to 300 psi. This verification actually consists of four activities: (1) reading the RCS pressure from an analog indicator; (2) reading a trip light indicating system status; (3) reading cooldown tables, which indicate reactor cooling over time; and (4) verifying that the information obtained from the

pressure readings and cooldown tables is consistent. A thorough sneak analysis would involve examination of each of these activities. For the purposes of illustration, however, we will consider primarily the reading of the RCS pressure.

Answering the second question (i.e., Can the operator see/hear the indication?) requires a human factors analysis of the facility. Factors such as illumination, ambient noise, size of markings of visual indicators, sound frequencies of audio indicators, and placement of the indicator relative to the operator will all impact whether or not the indication is available to the operator. Texts such as those written by McCormick and Sanders (1982) and Van Cott and Kinkade (1972) provide human factors design guidelines pertinent to controls and displays. These and other sources were used in the Sneak Analysis Tool to provide checklists, an example of which is shown in Figure 5, that provide resource material to the analyst conducting a human factors review. For each checklist question, "help" is available in defining criteria for proper evaluation. In the current illustration, inspection of the facility indicated that control room ergonomics were sufficient and that the operator should be able to successfully read the RCS pressure display.

Human factors analysis should also be useful in determining whether or not the operator misreads/mishears the indication (question 4). For example, an analog display, like the RCS pressure indicator in our example, is more likely to be misread than a status indication, like the trip light in our example.

Even if a display is not misread/misheard, the analyst must consider the possibility that the information read/heard will be misinterpreted (question 5). Factors such as operator training and procedures for the verification of information will impact the likelihood of misinterpretation. Here, misinterpretation is unlikely.

Note that the Sneak Analysis Tool presents questions in the appropriate logic structure, based on previous answers.

Sneak path. A sneak path exists in a human-machine interface when it is possible for the human operator to take actions other than those which are desired. Figure 6 is a flow diagram which guides the analyst through questions leading to the identification of possible sneak paths.

In our example, a sneak path would exist if valves other than D11-11/D11-12 could be used to achieve decay heat removal. Working through the flow diagram, then, we start by asking (A) is it possible to activate valves other than D11-11/D11-12 for D11R? Our schematic (Figure 3) shows that the system is not a single line node and that flow could also be established through local manually operated valves D11-21/D11-23. Thus, a sneak path may exist.

The actual presence of a sneak path, given a system that is not a single line node, is influenced by the presence or absence of barriers to the conduct of undesirable actions. Thus, the next pertinent question in our sneak path analysis is (B) are there barriers to prevent activation of valves D11-21/D11-23? Our schematic (Figure 3) shows that D11-21/D11-23 cannot be accessed from the control room. Only D11-11/D11-12, the desired valves, are remote motor operated valves. Hence, there is a design barrier to the operation of D11-21/D11-23 from the

control room.

Barriers eliminate the potential of sneak paths only if they cannot be circumvented. Thus, the final question in our sneak path analysis is (C) can the design barrier which prevents the operation of DH-21/DH-23 from the control room be circumvented? While it is not possible to physically manipulate DH-21/DH-23 from the control room, the operator does have the option of instructing someone outside the control room to initiate the opening of these valves. Hence, a sneak path exists if the operator exercises this option inappropriately.

Design features leading to sneak paths may be the result of desirable planned redundancies (i.e., to prevent failure of the primary system), as is the case in the current example. Thus, barriers to the use of sneak paths may be procedural rather than mechanical in nature. In the present case, such a procedural barrier might consist of instructions to the operator to never initiate manual opening of valves DH-21/DH-23 in the absence of a failure indication from the preferred valves unless maintenance or an in-service test of DH-11/DH-12 is planned.

Sneak label. The possibility of a sneak label occurs in a human-machine interface when labelled or symbolically coded controls are used by the operator. Coding of controls can be achieved through shape, texture, size, location, operational mode, and color, in addition to labels. As can be seen from Figure 7, the analysis of sneak labels is analogous to that of sneak indications, but controls, rather than displays, are the focus of attention.

In the ISLOCA example, sneak labeling is possible, as there are many controls available to the operator. However, control room ergonomics were found to be satisfactory, so labelling problems are probably not a great contributor to risk.

Sneak timing. As shown in the flow diagram in Figure 8, the possibility of sneak timing occurs in any human-machine interface in which the timing of human actions is critical to system performance. In our example, timing is critical because the procedure shown in Figure 2 indicates that valves DH-11/DH-12 should not be opened until RCS pressure drops below 300 psi. Opening the valves at a higher pressure can result in the ISLOCA.

From this point on, sneak timing analysis and sneak path analysis are quite similar, with the presence of adequate barriers playing an important role. Whether or not sneak timing can occur is influenced by the presence or absence of barriers to the untimely conduct of desirable actions.

In the ISLOCA example, sneak timing contributes significantly to risk, as opening the correct valves at the wrong time is the initiating event for the accident.

DISCUSSION

We began by suggesting that sneak analysis be used to generate inputs for HRA/PRA and specifically for identifying the top events in commission event trees. Because the output of a thorough sneak analysis is a comprehensive list of all possible sneak conditions, the methodology serves this purpose quite well.

It is obvious from the previous discussion that the human-factoring of instrumentation plays a large role in determining the magnitude of sneak conditions which exist in a system. It is difficult to imagine a complex human-machine system where sneak conditions are not possible -- the necessary use of multiple controls and displays in and of itself leads to the possibility of sneak conditions. However, the presence of human engineering design deficiencies which cause latent error conditions certainly increases the probability that a sneak condition will actually become manifest. Hence, correction of these deficiencies would be expected to have a palliative effect on system human error probabilities (HEPs).

Similarly, institutional procedures and training also have a great deal of impact on sneak conditions. Inadequate procedures and/or training will certainly increase the probability that operators take unplanned actions or act in an untimely fashion. In the DH valve illustration, for example, the institutional procedure of routinely jumpering valves in the DHR system increased the probability of premature valve opening over what it might have been had jumpering been subject to greater administrative control. Likewise, lack of awareness of the consequences of such actions, a training problem, also increased the potential for the act to occur. Again, enhancement of procedures and training may decrease HEPs by increasing the number of barriers standing between operators and inappropriate actions.

REFERENCES

- Reason, J. (1990.) Human error. New York: Cambridge University Press.
- Clardy, R. C. (1980). Sneak circuit analysis. In J. E. Arsenault & J. A. Roberts (Eds.), Reliability and maintainability of electronic systems. Rockville, MD: Computer Science Press (pp. 223-242).
- McCormick, E. J. and Sanders, M. S. (1982.) Human factors in engineering and design. New York: McGraw-Hill.
- Van Cott, H. P. and Kinkade, R. G. (1972.) Human engineering guide to equipment design. Washington, DC: American Institutes for Research.

Figure 2. Steps in initiation of decay heat removal.

Figure 4. Sneak indication flow diagram.

Figure 5. Sample Sneak Analysis Tool screens.

Sneak Indication Analysis

Must the operator obtain information
from an output source?

☒ **yes**

☐ **no**

Comments

The operator obtains information from three sources: RCS pressure is read from an analog indicator, a trip light indicates system status, and information is obtained from cooldown tables.

Use Checklist

Continue

Sneak Indication Analysis

Can the operator see or hear the indication?

☐ **yes**

☐ **no**

Comments

↑

↓

Use Checklist

Continue

Sneak Indication Sample Checklist

Return

Click on any question for more information.

Does the operator have sufficient corrected or uncorrected visual acuity to see normal visual inputs?

☐ ☐ ☐
yes no n/a

Does the operator have sufficient ability to perceive colors to see normal visual inputs?

☐ ☐ ☐
yes no n/a

If the operator must view inputs in darkness, is sufficient time allowed for dark adaptation?

☐ ☐ ☐
yes no n/a

Sneak Indication Analysis

Can the operator see or hear the indication?

☒ **yes**

☐ **no**

Comments

Human factors analysis indicates that the operator should be able to see the indicator.

Use Checklist

Continue

Sneak Indication Analysis

Does the operator misread/mishear the indication?

☒ **yes**

☐ **no**

Comments

With an analog indicator, there is some probability of misreading.

Use Checklist

Continue

Sneak Indication Analysis

Does the operator misinterpret the indication?

☐ **yes**

☒ **no**

Comments

The indicator is not likely to be misinterpreted.

Use Checklist

Continue

A: Is it possible for the operator to take actions other than those which are desired?

B: Are there barriers to prevent the operator from taking undesired actions?

C: Can the barriers be circumvented?

Figure 6. Sneak path flow diagram.

A: Is the timing of the operation critical?

B: Are there barriers to prevent untimely actuation?

C: Can the barriers be circumvented?

Figure 8. Sneak timing flow diagram.