SAN097-2622C
SAND--97-2622C

Human Factors in High Consequence Manufacturing Systems

CONF-971170--

Chris Forsythe and Eric Grose
Statistics and Human Factors, Sandia National Laboratories, MS 0829, Albuquerque, NM 87185-0829, USA

A high consequence system is often defined as one in which the potential exists for severe or catastrophic accidents. Familiar examples include nuclear power plants, airline and other mass transportation, dams and reservoirs, and large-scale food processing. Many manufacturing systems also qualify as high consequence systems.

Much of the authors' experience with high consequence systems derives from work associated with the surveillance and dismantlement of nuclear weapons for the United States Department of Energy. With such operations, there exists a risk of high explosive detonation accompanied by radiological dispersal and, potentially, nuclear detonation.

Many common facets of manufacturing systems may contribute to their having the potential for high consequence accidents (e.g., explosive materials, flammables, extreme high and low temperatures, high voltage, high energy mechanical elements, toxic chemicals, gases or materials, etc.). In addition, the definition of high consequence may be expanded to encompass monetary losses, lost productivity, property damage, and injury to a company's reputation and status. If a major fire leads to substantial economic losses due to destruction of goods, equipment and facilities, and the subsequent loss of productivity, there may be no loss of life, but severe consequences for the proprietors, their employees and the surrounding community. Furthermore, with mass production, undetected manufacturing process errors may be replicated in large numbers resulting not only in economic losses, but irreparable damage to the company's reputation among consumers.

Analysis of major industrial accidents such as Three Mile Island, Chernobyl and Bhopal have revealed that these incidents were not attributable to a single event or direct cause, but were the result of multiple factors that combined to create a condition ripe for an accident (Sudano, 1994). In each case, human error was a critical factor contributing to the accident. Consequently, many authors have emphasized the need for greater appreciation of systemic factors and in particular, human activities (Greatorex & Buck, 1995; Woods, 1990). This paper discusses approaches used in hazard analysis of U.S. nuclear weapons operations to assess risk associated with human factors.

Understanding and Preventing Accidents

Two things must be understood about high consequence events. First, they are rarely the result of a single large failure, but the combination of many small failures (Woods, 1990). In general, this testifies to the success of engineering approaches in reducing the risk of catastrophic events attributable to single-point failures. It also suggests that within complex systems, there may exist vulnerability to many subtle

DISCLAIMER

modes of failure. Second, high consequence events tend to result from unique permutations of events that defy prediction of their exact make-up. However, certain attributes of a high consequence event may be highly predictable from an understanding of system vulnerabilities.

Understanding the risks within a complex system may begin with identification of hazards that are present. A good point to start is with a general consideration of *what energetic substances are present*? With this knowledge, process steps may be reviewed to identify where actions have the potential for initiating energetic release. Similar questions might address *what energy sources are available, or what materials are present and what risks might they pose*? The point of these analyses is to conduct a systematic review that identifies vulnerabilities within a system.

Once cognizant of the hazards, the specific methodology applied may vary. For instance, fault trees may be used to derive combinations of basic events that lead to specific accidents (see Figure 1). Here, one works backwards from the accident to determine the chain of events or combinations of events sufficient to produce the accident. In contrast, event trees may be used to extrapolate possible accident scenarios from basic events (See Figure 1). Following this approach, one first asks what might go wrong at a given point and then, speculates on what might happen if it were accompanied by other failures.

There are many analytic possibilities and whichever is employed, the result should be a collection of events that contribute to accident scenarios. An important point to remember is that no event, in itself, may be particularly worrisome. The history of disasters suggests that they are rarely attributable to a specific cause, but instead, result from the combination of many small events. The goal is to assure prevention of highly salient modes of failure, as well as less consequential events that, under the right circumstances, may contribute to a high consequence event.

Positive Controls

The prevention of accidents occurs through control of events that could contribute to an accident. To discuss controls, three terms should be defined:

Risk State - condition in which potential exists for the occurrence of an event that may lead to undesired consequences

Event - occurrence of the potential for undesired consequences

Consequence - results, such as injury, death or loss, whose potential defines the presence of a risk

For the example shown in Figure 2, an open electrical circuit (the risk) would create a condition in which there existed a potential for contact (the event) and given contact, a potential would exist for electric shock (the consequence).

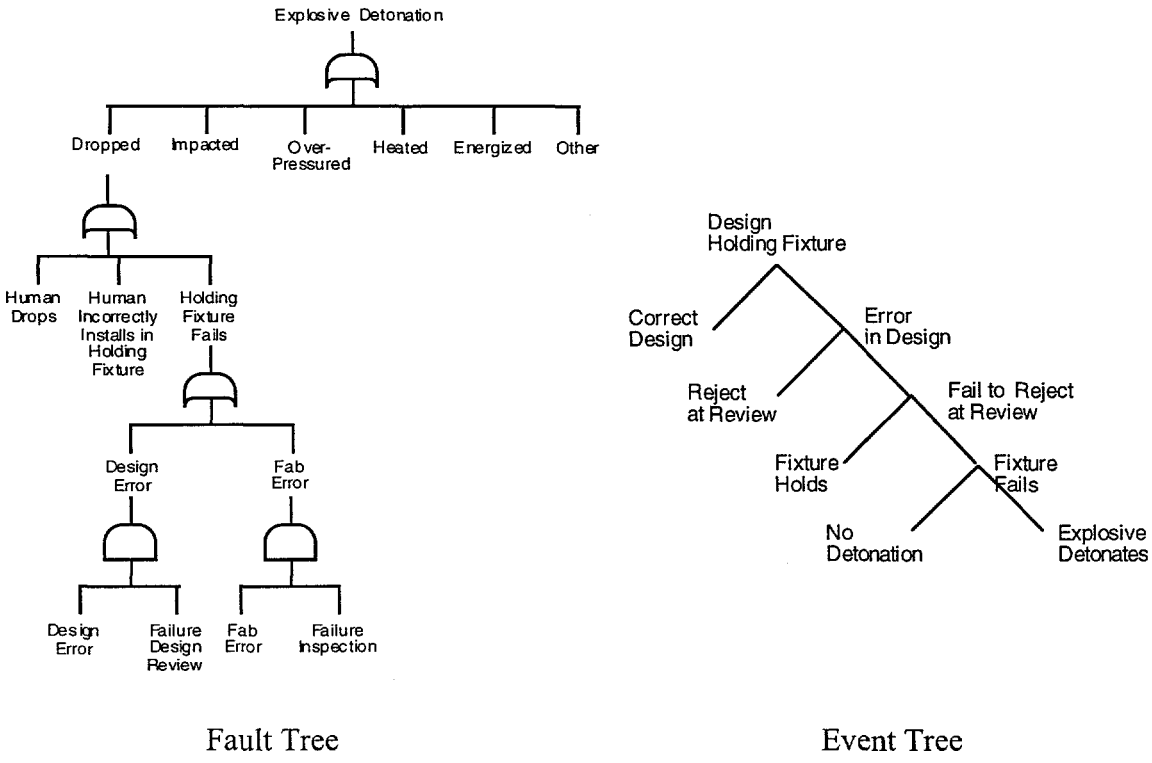

Figure 1. Illustrates the Use of Fault Tree and Event Tree Approaches to Understand the Sequence of Events Leading to an Accident

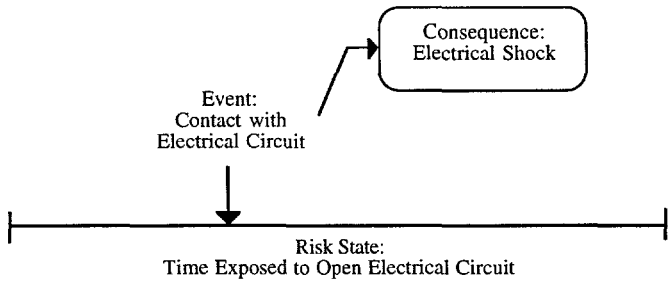

Figure 2. Graphic Depiction of the Relationship Between Risk State, Event and Consequence.

Controls may operate as follows:

- Prevent Occurrence of Risk State (e.g., if electricity is excluded, electric shock is precluded)

- Given Occurrence of Risk State, Reduce Exposure to Risk State (e.g., minimizing the number and distance of explosive hand carries reduces exposure to the potential for dropped explosive)

- Given Exposure to Risk State, Reduce Potential for Event (e.g., if slip hazard is present, non-slip surface would reduce potential for slip)

- Given Event, Reduce Potential for Consequences (e.g., minimizing drop heights for explosive would reduce potential for explosive detonation following a drop)

- Given Consequences, Reduce Magnitude of Consequences (e.g., performing manipulation of small quantities of explosives behind a Lexan shield could reduce consequences of an explosive detonation).

For each identified event that could contribute to an accident, there are likely to be one or more controls in place. However, one must ask how adequate are those controls and do they provide an acceptable level of assurance?

Adequacy of Controls

Two additional terms need to be defined in regard to controls:

Effectiveness - when functioning as designed, ability of the control to act through any mechanism (preventing risk state, lessening potential for events, etc.) with the end result being a lessening of the potential for consequences

Reliability - the potential for the control to be present and operational, as opposed to an absence of the control, whether by physical absence or an absence of specified response

Consider the scenario in which a vibration event leads to structural failure of a high-velocity centrifuge. An out-of-balance sensor capable of automatically shutting-down the centrifuge if a relatively low out-of-balance threshold is exceeded may serve as a control. For this example, effectiveness would refer to the ability of the out-of-balance sensor to detect instances of vibration. Reliability would address the likelihood that the sensor, shut-off and associated circuitry operates properly once a vibration-induced, out-of-balance event occurs.

Any given control may be placed within the plot shown in Figure 3. To illustrate, consider a relatively simple event: a fixture comes loose from a high-velocity centrifuge

due to incorrect installation. Figure 4 shows how some common controls might be assessed. *One-Way Installation* provides both an effective and reliable control that, in itself, may be judged adequate. None of the remaining controls provide nearly the same level of effectiveness or reliability, and given the consequences of a fixture coming off the centrifuge while in operation, it is questionable whether any of these controls alone or all in combination would be adequate.

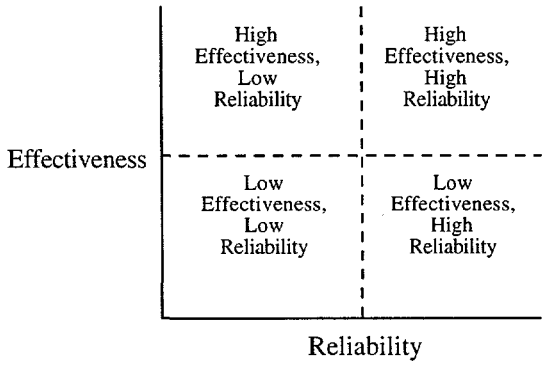

Figure 3. Controls Have an Associated Effectiveness and Reliability

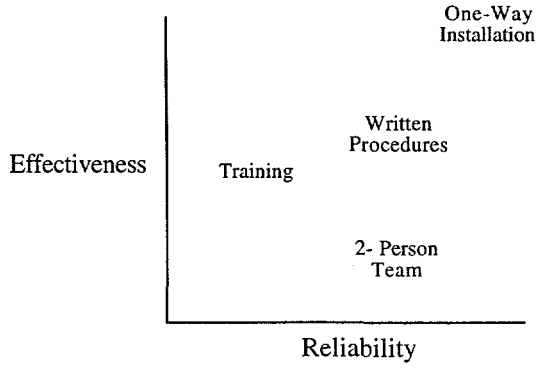

Figure 4. Ratings of Controls for the Event of a Fixture being Misinstalled on High-Velocity Centrifuge

The adequacy of controls may be judged on the basis of their effectiveness and reliability. The authors have had success with an approach whereby the questions of effectiveness and reliability are reversed. Instead of asking how effective or reliable is the control, one asks in what ways is the control lacking effectiveness or reliability. The goal is to account for deficiencies in effectiveness and reliability, or as shown in Figure 5, explain what would be necessary to fill-in the gaps. The benefit of such an approach is that the natural outcome is suggestions for how to improve the effectiveness and reliability of controls.

Positive Control of Human Error

With any accident, it is nearly certain that human error will be a contributing factor. As the fault tree in Figure 1 illustrates, the human error may occur downstream (e.g., production worker drops explosive) or upstream (e.g., error in design of explosive holding fixture by tooling engineer). Two distinct types of controls are employed for human error. Engineered controls are those which preclude human error through design. For example, a tool is designed so that it can only be installed in one direction or a torque limiter is incorporated that prevents over-tightening. In contrast, administrative controls seek to prevent human error through measures such as written instructions, warnings, labels and training. Administrative controls are inherently weak. As shown in Figure 4,

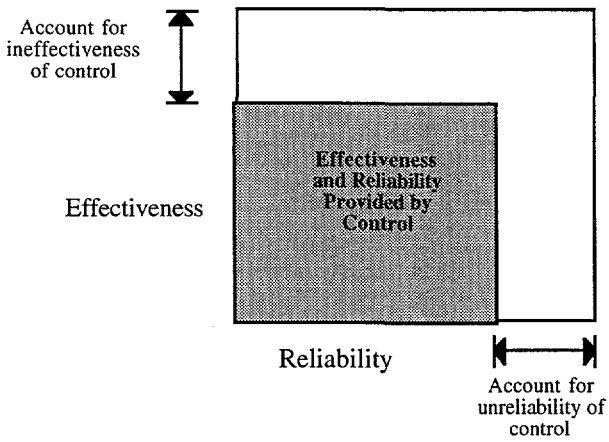

Figure 5. Judgment of the Adequacy of Controls Based on Understanding Why Controls Fail to Provide Complete Effectiveness and Reliability

neither their effectiveness nor reliability is comparable to that obtained with engineered controls. To illustrate this point, a brief review of incidents reported in the Office of Nuclear and Facility Safety's *Operating Experience Weekly Summary* was conducted. Of forty incidents, twenty could be directly attributed to a failure of one or more administrative controls. In contrast, only four incidents could be attributed to a failure of an engineered control. Despite the inherent weakness, reliance on administrative controls is pervasive.

Unfortunately, while the application of engineered controls may push the occurrence of human error upstream, a point is reached where administrative control cannot be avoided. One-way installation of tooling may preclude error on the shop floor, but no comparable control exists to prevent an error by the designer of the tool. By necessity, reliance must be placed on independent design reviews, and design verification and validation processes. The important point is that where engineered controls are not feasible, care should be taken to maximize the effectiveness and reliability of administrative controls. This may be accomplished through strategies that emphasize redundancy and independence. There should be multiple opportunities to recover should an error occur and should an error recovery mechanism fail, its failure should not influence performance of other error recovery mechanisms. Within an engineering environment, multiple reviewers provide redundancy. A review process wherein reviewers have no stake in the design, and limited interaction with designers and other reviewers while performing the review provides independence.

Safety Culture

A common practice of many institutions concerned with safety and accident prevention has been to plaster the walls with safety slogans and require workers to attend mandatory safety training. While reasonable if implemented as part of an overall strategy of *defense-in-depth*, very little improvement should be expected from these practices alone. Improvements are realized when efforts are undertaken to maximize the effectiveness and reliability of controls. However, cultural barriers may significantly impede such efforts. For example, a cultural predisposition to favor administrative controls (e.g., adherence to written instructions, and training) often produces an environment where workers are blamed, and sometimes punished, for errors that could have been precluded through well-placed engineered controls. Organizational dynamics may make it politically advantageous to either exclude or devalue the input of adversaries who might otherwise offer a valuable error recovery mechanism. Furthermore, a failure to properly appreciate and prioritize safety at any level in an organization may encourage the expedience of inaction.

Without removing cultural barriers to safety, good intentions are rarely sufficient. No one, in good conscience, wants to see an accident. However, people vary in the lengths to which they will go to avoid accidents. The issue of how employees may be motivated to adopt conscientious attitudes toward safety goes beyond the bounds of this paper. However, given such motivation, the approaches outlined in the preceding sections suggest certain cultural attributes. These would include: (1.) an unwillingness to accept any hazard, no matter how insignificant, unless adequately controlled; (2.) a reliance on administrative controls ONLY when engineered controls have been thoroughly exhausted; and (3.) an acknowledgment of the potential for error and the institution of effective and reliable error recovery mechanisms.

Conclusion

Disasters are rarely the result of a single initiating event. Instead, they are typically attributable to a combination of factors. Thus, safety within high consequence systems relies on the control of numerous potential events, many of which may not be particularly threatening in isolation. To provide assurance, a control must be effective and reliable. Engineered controls typically provide far greater levels of effectiveness and reliability than do administrative controls. However, administrative controls are valuable when treated as components within an overall defense-in-depth safety scheme.

Acknowledgments

This work was supported by the United States Department of Energy under Contract DE-AC04-97/AL85000.

References

Greatorex, G.L. & Buck, B.C. (1995). Human factors and systems design. GEC Review, 10, 176.

Sudano, J.J. (1994). Minimizing human-machine interface failures in high-risk systems. IEEE Aerospace and Electronic Systems Magazine, 9, 17-20.

Woods, D.D. (1990). Risk and human performance: Measuring the potential for disaster. Reliability Engineering and System Safety, 29, 387-405.