ABSTRACT

Safety is of paramount concern in today's high technology environment. Because of technological advances, there are numerous situations (high consequence operations) for which the implications of a safety failure are so severe that extreme attention to safety systems is essential. Some of those situations are: nuclear weapon detonation safety, nuclear reactor safety, dam safety, mass transit transportation safety, and hazardous materials transportation and handling safety. In each case, specific safety systems, human control, and administrative procedures have been designed to give a high level of assurance against disasters.

In an overview sense, safety concepts can be divided into two broad approaches: active safety and passive safety. Active safety systems, in general, are based on the need for "functioning" elements (operating motors, operator action, etc.) and safety may be based in a large measure on "reliability" data (historical records of the operability success of components). Passive safety basically depends on non-functionality.

Active safety systems are the most widely used and best known types. However, passive safety can be an important contributor to the safety of systems having critical functions. For example, the prevention of inadvertent detonation of nuclear weapon systems is based on passive safety features, implemented in conformance with strict "first principles" that are chosen based on fundamental physical relations.

One of the reasons for the prevalence of active-safety systems is that there is a common human tendency to embark on a design/implementation that will "accomplish" safety. Humans are generally more inclined to think about how to make components work right than to think about what might keep components from working wrong. While passive safety is not applicable to many situations (e.g., the safety of a flying aircraft must be strongly dependent on active safety\(^1\)), the role of passive safety is important to consider, and its utility to achieve very high levels of assured safety is receiving increased attention.

In this paper, some background on safety implementations and safety assessment methodology are reviewed, the salient features of passive safety implementations are demonstrated, and some applications for which passive safety is particularly appropriate are suggested. Included are requirements on components and processes, and design principles. Critical agents (humans, stress, equipment, and timing) are some of the pertinent factors considered.

Background

Figure 1 illustrates that the safety of critical operations can be partitioned into an active and a passive regime. Although active safety systems may have a passive safety element, they basically depend on continuously functioning equipment or on some intervention action to maintain safety. The active response requires that the need for intervention be detected and that there be a reaction. This can be accomplished by human response or by automated equipment, or combination of the two. However, both of these forms of action have the potential to be relatively unreliable. For example, human reaction may be required under extremely challenging circumstances, where time available may be limited and the stress placed on the human to act correctly may be high. Automated equipment response is also challenging, since successful safety system operation is often required within short time frames, and must take place at the same time (and in the same environment) in which failures are occurring (the failures being the causes of the safety problem or hazard).

In contrast, passive safety is built into systems without urgency, allowing for effective requirements, the incorporation of firm principles in design, production controls to assure no compromises in the actual implementation, overall process reviews and controls. In addition, testing and experience can be gained. Maintaining effectiveness over time can be assured by surveillance and maintenance to prevent deterioration as items age.

This work was supported by the United States Department of Energy under Contract DE-AC04-94AL85000.

\(^1\) Systems such as aircraft can incorporate both active and passive safety features.
DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.
Quantitative vs. Qualitative Safety Assessment

Performance-based assessment tools, such as PRA (probabilistic risk assessment) are well known and widely used in the safety assessment of systems based on active safety. Passive safety assessment can utilize the same set of logic models and tools, but heavy emphasis is placed on principle- and physical-law-based engineering models, detailed production controls, and metrics which draw on these sources. The traditional reliability database (on which traditional PRA has a heavy reliance) is not either available or necessarily applicable.

As an example, the Golden Gate Bridge provides safety to automobile passengers moving across it, giving assurance that in the absence of some dramatic action (e.g., an unprecedented-magnitude earthquake, etc.) the passengers will be safe (as will those in the shipping lanes below). The bridge safety depends on following principle-based, well understood design rules, by allowing reasonable error- and uncertainty-tolerance margins, and incorporating a constant surveillance and maintenance program to maintain the initial design/fabrication intent. Once these passive safety features have been incorporated, analysis of "the probability of safety failure" is relatively meaningless. Some statistical earthquake data, and some human performance modeling could be used to estimate the risk probability, but these are not the kind of accurate predictors that are necessary for a meaningful PRA, even one with uncertainty measures.

The contributions of analytical models such as those used in PRAs are to give greater qualitative understanding of the effects of various system factors and to facilitate focusing on significant areas in a cost-efficient manner. Sensitivity analysis, cutset identification, and uncertainty analysis are significant contributors to this understanding. There is often a temptation to generate numeric PRA measures from weakly known input data. The danger is that the quantitative outputs may be given more credence than the understanding of inputs justifies. This is frequently the case when PRA is attempted for passive-safety-based systems. A preferable approach is to lay out the structure of a safety "theme," in which the designer clearly identifies the features, and only those features, that are intended to meet the safety objective. This includes the principles on which the theme is based, identification of "safety-critical" components and requirements for the performance of those components, and a process for controlling the design, production, and maintenance of these components, including periodic assessment reviews.

Testing

Active safety systems can be partitioned into two categories: automated systems and human systems. Passive safety systems can be partitioned into "no-response" systems and systems where only properties change, as shown in Figure 2:
One of the most critical safety requirements for the nation is that nuclear weapons be unlikely to detonate accidentally, no matter what accident or environment might occur. First, extraordinary measures are taken to minimize the likelihood of an accident, but in addition, the weapon safety design is based on the assumption that an accident has occurred, and very high levels of engineered safety must be provided, given the accident. To meet this challenge, passive safety features are implemented rather than active safety features (features for which an operation must take place to assure safety). Safety is then based on components for which behavior depends on engineered basic principles. This concept avoids safety based solely on analysis of system components without a stringent a-priori system and component safety design, requirements, and review strategy.

These are the basic keys to modern nuclear weapons detonation safety. The concept is described below, along with background on control factors and assessment approaches.

The safety theme for nuclear weapon detonation safety is based on the principles of "isolation," "inoperability," and "incompatibility," all of which are passive safety principles. Without going into specific design details, weapons provide a nuclear yield only when detonated in response to a particular type of high voltage electrical energy. Modern nuclear weapons detonation safety is based on isolating that energy from critical living components, which are located in an "exclusion region," protected from outside sources by a robust "barrier." This exclusion is the principle of "isolation," which is implemented by carefully designing the barrier structure, using materials and processes in conformance with well understood properties.

In order for the weapon to operate when intended, there must be the capability to provide the critical energy to the critical components in the exclusion region (and preclude the energy in accident environments). This function is implemented in nuclear weapon systems by a "stronglink switch." The switch is a gateway which acts as a barrier until a human decision is made to remove the barrier. Electrical energy is allowed to pass through the exclusion region barrier only after an unambiguous stimulus (indication of intended use that is extremely unlikely to be inadvertently created by any process, including abnormal environments) is provided. Then the switch will operate and allow electrical energy to pass through the barrier.

The stimulus is provided by a "unique signal," which comprises a series of "events" introduced into the weapon system by human action, with each event communicated separately from a source to the
stronglink switch. Each event is generally one of two types, and the sequence of events (the "pattern") is engineered for maximum "uncertainty" (minimal predictability). The strategy of generating and delivering this stimulus is done in consonance with the principle of "incompatibility" (using a stimulus that is incompatible with other feasible stimuli). The incompatibility principle is supported by "independence" and "uncertainty." The process is designed to accept separately communicated inputs, because separate sequential inputs from inadvertent processes that might be received are more likely to be independent. The safety assurance inherent in communicating a sequence of events depends on this independence.

The purpose of the engineered pattern is to make it extremely unlikely that any naturally occurring (or accident-generated) process would duplicate the pattern. The number of patterns that provide acceptable uncertainty is small, because there are stringent requirements placed on the pattern properties. The combination of communication technique and pattern uncertainty provides the unique signal incompatibility.

Since no barrier can survive all possible "abnormal environment" situations, the isolation principle must be combined with the principle of "inoperability," where some component that is critical to the nuclear detonation process will predictably fail (become inoperable) in environments less severe than those that can cause isolation to fail. This depends on co-locating robust isolation features with "weak-link" inoperability features so that they will be exposed to the same environments. This implementation strategy must be supplemented by demonstrating to independent assessment teams the nature of the safety theme, the identification of safety-critical components, and that the implementation supports the requirements and principles.

Conclusions
Passive safety is an important capability for systems operating in a high consequence environment. The advantages of true fail-safe performance, principle-based implementation, and process control over the system lifetime can be important safety contributors. In addition to the direct benefits, passive safety also minimizes the need for analysis and testing of components and systems that are not part of the safety theme. The assurance process depends on proper design and manufacturing controls and minimizes/eliminates the vulnerability to functional operations to achieve high consequence safety. Although it is recognized that passive safety concepts are not universally applicable, their use should be considered wherever it is feasible.

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.