SAND91-1269

THE UNIQUE SIGNAL CONCEPT FOR DETONATION SAFETY IN NUCLEAR WEAPONS

UC-706

System Studies Department, 331

Sandia National Laboratories

ABSTRACT

The purpose of a unique signal (UQS) in a nuclear weapon system is to provide an unambiguous communication of intent to detonate from the UQS information input source device to a stronglink safety device in the weapon in a manner that is highly unlikely to be duplicated or simulated in normal environments and in a broad range of ill-defined abnormal environments. This report presents safety considerations for the design and implementation of UQSs in the context of the overall safety system.

December 1992

ACKNOWLEDGEMENT

Beginning in the early 1970s, the Sandia Laboratories Nuclear Safety organization began investigating approaches that culminated in the unique signal concept. The development has involved a large number of Sandians, with significant early contributions from Stan Spray, Wally Crammond, and Jay Grear. The thought processes were also enriched by a number of persons outside Sandia. The original draft of this report was prepared by Curt Mueller; the final version was the responsibility of Stan Spray and Arlin Cooper.

TABLE OF CONTENTS

Chapter I

THE UNIQUE SIGNAL CONCEPT

Introduction

To help assure predictable nuclear detonation safety in a broad range of ill-defined abnormal environments, the safety concept of the unique signal (UQS) was developed. The purpose of a UQS in a nuclear weapon system is to provide an unambiguous communication of intent to detonate from the UQS information input source device to the stronglink safety device in the weapon such that the likelihood of normal or abnormal environments duplicating or simulating the UQS is vanishingly small. Thus, the UQS serves both a reliability function and a safety function. The reliability function of the UQS is to permit prearming for a detonation when that is desired and authorized. The safety function of the UQS is to maintain safety assurance of the weapon system at all other times, including accidents and other abnormal environments. The UQS's safety function is the subject of this report.

The safety goal of the UQS is to assure by first-principle design that the likelihood that accident-generated inputs might simulate the UQS from the intended source is much less than the likelihood that safety devices will fail to isolate energy in abnormal environments and that the quantitative level of system safety meets national standards. This approach is necessary to help compensate for the unknown and unknowable response of UQS communication channel equipment in abnormal environments, and to reduce this contribution of the likelihood of failure to a very low quantitative level.

It is impractical to electrically isolate weapon prearm/safing switch actuation lines from electrical sources in abnormal environments. Instead, an "incompatibility" safety principle is employed: safety-critical signals are transmitted in the form of UQSs. An important benefit is that the UQS communication channel does not have to be designed, analyzed, or tested for a safe response to abnormal environments if there is no resident unique signal knowledge (i.e., no UQS pre-storage and no multiple-event buffering, both discussed subsequently); only the UQS information source input device and the stronglink safety device in the weapon must respond in a predictably safe manner in abnormal environments.

Non-Random Response of Weapon Systems to Abnormal Environments

First, we will examine how one might realistically characterize the response of weapon systems to abnormal environments, which may range from the mild (such as a power supply running slightly out of specification) to the severe (such as an airplane crash and fire).

It would be easy to assume that nature is "random", meaning that all possible outcomes are equally likely and independent. However, the design for a weapon system will incorporate features which create biases -- that is, tendencies toward certain responses -- in the system's behavior in

abnormal environments.

A few examples of design features that can bias response to abnormal environments are:

- Conductor assignments in cables
- Choices of materials
- Printed wiring board layouts
- Computer programming algorithms
- Etc.

The designed-in tendencies toward certain responses created by such design features are not random, that is, they are neither equally likely nor independent. While it is not uncommon for safety analysts in certain types of situations to assume random threats, it is clear that abnormal-environment nuclear safety analysis can afford no such simplifications.

Except for identified weapon system safety features such as stronglinks and exclusion region barriers, it is not practical to carefully design, analyze, test, and control components and systems in production as would be required to establish the properties in abnormal environments. To do so for just the initial design would be prohibitively expensive, while keeping up with modifications and additions would compound the complexity. Avoidance of such a necessity is one of the primary goals of the UQS concept. Thus, the biases potentially existing in a large part of a weapon system are not known and, in a practical sense, cannot be determined. Such unavailable information is often termed "unknown and unknowable". However, unknown and unknowable in no way implies random.

The objective must be to engineer a UQS that is not susceptible to unknown and unknowable, but not necessarily random, biases in the response of weapon systems to abnormal environments; and in doing this, to minimize/eliminate the criticality of major parts of the system to nuclear detonation safety.

The Role of Uncertainty in a UQS

The approach that has been taken to meeting that objective is to introduce uncertainty into the UQS. That is, the UQS is designed to require an "unintended generator" to perform in an uncertain manner if it is to generate the correct UQS. The goal is to assure that the worst case for an unintended generator is randomness, and to achieve the goal through design, not through assumptions. If there are any tendencies toward repeatable behavior, they must decrease the likelihood of generating the correct UQS.

Uncertainty is introduced into the UQS by requiring change between at least two different conditions. The choices an unintended generator must make as to whether to change or to repeat offers the opportunity to design in uncertainty. As will be seen, because of the uncertainty engineered into UQSs, a broad range of unintended generators incorporating biases can be made less likely to generate a correct UQS than a truly random generator.

Structure of a UQS: A Sequence of Events

To be viable, the UQS concept implies that the UQS pattern itself must be carefully engineered to assure there is a very small likelihood of the correct UQS being inadvertently generated in a broad range of ill-defined abnormal environments. A major goal of the UQS concept is to make this likelihood as small as required so that engineering efforts can concentrate on preventing premature application of the UQS by the intended source in abnormal environments in the absence of human action, and on preventing premature operation of the weapon abnormal-environment-resistant safety device (stronglink) in abnormal environments in the absence of the UQS.

The first step in engineering a UQS that meets this goal is to establish its structure. However, it must be recognized that, in addition to meeting the nuclear safety goal stated in the preceding paragraph, the structure selected for a UQS should also accommodate certain practicalities. Three major practical considerations influenced the structure eventually chosen for UQSs. First, it must be possible to design and build reliable, abnormal-environment-resistant UQS stronglinks that are capable of discriminating the UQS from all other potential inputs. Second, the UQS must be amenable to communication over a wide variety of channels, ranging from analog on a single wire through digital systems. Non-electrical UQS communication channels, such as mechanical (e.g., push/pull on a rod or cable) and optical should also be accommodated. And third, it must be possible to design and build UQS input mechanisms that meet both nuclear safety and reliability/operability requirements.

In order to both achieve the nuclear safety goal and accommodate these practical considerations, the structure selected to be employed in all UQSs is that of a sequence of unrelated and unrelatable events with each UQS event in turn being applied at the information source device interface, transmitted through the UQS communication channel, and responded to by the stronglink's UQS discriminator. The UQS discriminator must be carefully designed, analyzed, tested, and controlled in production to assure that it will respond to each UQS event as it is received from the UQS communication channel (only one event at a time) in both normal and abnormal environments; the UQS communication channel (Chapter III) must be utilized in a matter to assure that it communicates only one UQS event at a time from the UQS source to the stronglink's UQS discriminator; and the UQS source at the information source input device interface (Appendix AI) must be designed to apply only one UQS event at a time to the UQS communication channel.

The reason for selecting the structure of a sequence of unrelated and unrelatable events for the UQS -- and for designing, analyzing, and testing the safety subsystem to assure that this structure is maintained -- is to provide a method of communication that is both analyzable and predictable in abnormal environments. As a result of extensive study and analysis in which a number of possibilities were examined over a period of several years, only a soundly engineered pattern of a sequence of unrelated and unrelatable events has been found to be amenable to analysis incorporating a realistic treatment of abnormal environments.[1]

[1]Some other approaches that have been studied and rejected due to significant weaknesses are mentioned in Appendix AII.

A Visualization of a UQS

A UQS process may be visualized as the equivalent of a multiple-step maze. As shown in Figure I-1, the UQS affords a sequence of simple choices, and each and every simple choice must be correct to reach the end of the maze. If any of the simple choices is incorrect, the route taken through the maze leads to a dead end. Unlike conventional mazes, travel in the reverse direction is not permitted; therefore, just one step into a dead end -- a single incorrect choice -- results in lockup in a safe condition.

The (independent) "choice of direction" at each "step in the maze" is called an event. The sequence of events required to travel through the maze is called the pattern and must be engineered to be highly unlikely to be duplicated or simulated in a broad range of ill-defined abnormal environments. Thus, the UQS is a sequence of independent events in a specified pattern. Each individual event represents a simple choice; no attempt is made to preclude the generation of events in an accident. The safety of a UQS is wholly based on the unlikelihood that its pattern (one specific engineered sequence of events) will be sequentially generated (one independent event at a time) in abnormal environments.

To maintain the desired uncertainty and independence, the steps in the maze must be taken one at a time in order. Each communication should relay only the choice of direction for the next step in the maze, not a "road map" to multiple steps.

In reality, an electro-mechanical equivalent of the conceptual multiple-step maze must be embodied in the stronglink's UQS discriminator. In the system's normal-environment reliability mode, the UQS communication channel transmits separate instructions (events) from the information source input device interface to the UQS discriminator specifying the "choice of direction" for each sequential "step in the maze". In abnormal environments, events can appear at the stronglink from a wide variety of unknown and unknowable sources.

In both normal and abnormal environments, the stronglink's UQS discriminator accepts a sequence of events, one event at a time, and makes a judgment as to the correctness of each event in turn. If an incoming event is correct for that event in the sequence, the UQS discriminator advances one event position and waits for the next incoming event; if an incoming event is incorrect, the UQS discriminator locks up in a safe condition. Inputs that are not recognized as either correct or incorrect are called "non-events," and result in no discriminator action. Any input to the stronglink's UQS discriminator results in an advance of one position at some events in the sequence and lockup at other events is defined as a UQS event. All other inputs to the UQS discriminator (and correspondingly in the communication channel) that result in no discriminator action are called non-events.[2]

[2]"Non-events" are discussed later in this chapter.

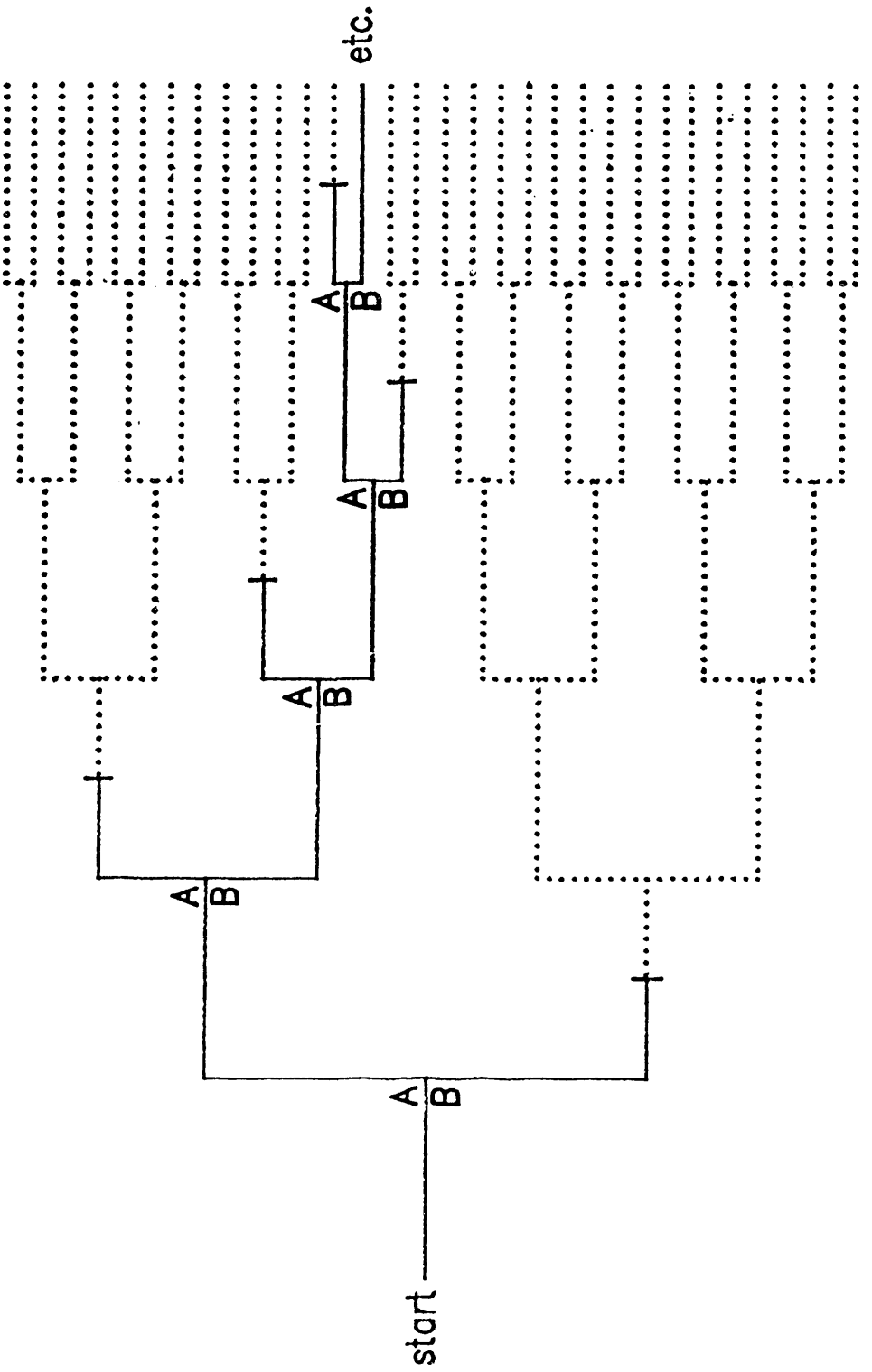


Figure I-1
A Visualization of a UQS as a Multiple-Step Maze

The "Pattern" of a UQS

In the context of UQSs, the word "pattern" has a very specific definition. A UQS pattern refers to the sequential order in which the events of a UQS appear. Any sequence of events expresses a pattern. The one specific sequential order of events necessary to enable a stronglink device is called the pattern of its UQS. In a typical implementation, a representation of the pattern of the UQS is stored in steel teeth in the stronglink's UQS discriminator. No other pattern may enable the UQS device. The pattern of a UQS is safety-critical and is usually fixed (non-changeable) and non-secure (unclassified).

Some potential patterns are less likely to be generated in abnormal environments than others. The topic of engineering patterns suitable for use in UQSs in nuclear weapon safety devices is discussed at length in the next chapter.

The UQS "Event" and Its "Format"

Like the word "pattern", the words "event" and "format" have very specific definitions in the context of UQSs. The word "event" refers to one independent element of a temporal sequence.

Each UQS event is separate from and unrelated to the other UQS events in the sequence. The dictionary definition of event, "something that happens", is appropriate in that each UQS event happens by itself at a different time from and unrelated to all other UQS events.

The information communicated by a UQS event is the choice of direction for just one step in the conceptual maze. In all current and past implementations of UQS discriminators for stronglinks, only two possibilities exist for each choice.[3] Therefore, only two UQS event types need to be supported by the UQS communication channel. For convenience, the UQS event types are labeled alphabetically, e.g., an 'A' event type or a 'B' event type -- or 'C' and 'D' to distinguish them from UQS events intended for other stronglinks. However, '0' and '1' are not used as identifiers for UQS event types to avoid confusion with digital bits.

Each UQS event can be communicated using some representation such as digital (two bits, two words, two messages) electrical (e.g., two levels of DC voltage, two pulse durations, etc.), mechanical (e.g., push/pull strokes on a stiff cable), optical, or pneumatic. Other energy forms are possible. Although the discussions in this report may, on occasion, allude to electrical forms, the discussions are applicable to other energy forms as well.

In the UQS context, the word "format" specifically refers to the description, including all tolerances, that defines a UQS event type, i.e.,

[3]Theoretically, a stronglink discriminator could be designed with more than two possibilities for each choice. However, the length of the UQS sequence required to meet safety considerations as presented in Chapter III could be shortened only slightly, not justifying the increased complexity of the discriminator mechanism.

'A' or 'B'. Intentionally delivered formats in normal environments are usually tightly controlled, but acceptance tolerance may be wide. In abnormal environments, the format chosen for an event is not safety-critical because it communicates only one simple choice (UQS event type). Within the UQS communication channel, it can be represented in any applicable manner (e.g., 28v DC pulses, digital messages, optical signals, etc.).

For convenience within the UQS communication channel, one format can be translated to any other (e.g., digital message to DC voltage pulses) as long as it's done one UQS event at a time. Thus, the same 'A' type UQS event may be represented by different formats at different points in the UQS communication channel. Different formats must not be created for different event positions in the sequence, because to do so would violate the independence concept. However, format tolerance (tolerance to uncontrolled or uncontrollable variations) can be broad.

Tolerances in both the stronglink's UQS discriminator and in format translators in the UQS communication channel will allow variation in the UQS event formats (e.g., inadvertently generated) to which the discriminator will respond. That is, at any given point in the UQS communication channel, a variety of formats can all result in an 'A' UQS event type response by the UQS discriminator, and another group of formats can all result in a 'B' response. Furthermore, the range of formats representing a given UQS event type may be altered in abnormal environments. From the safety standpoint, it makes no difference whether the tolerance bands on UQS event formats are tight or broad. All format variations that result in an 'A' response by the UQS discriminator are equivalent and are, by definition, 'A' event types; there is no preference one over another. Likewise, all format variations that result in a 'B' response by the discriminator are 'B' event types. However, discrimination must be designed to remain consistent through the sequence. That is, if a format is chosen for an 'A' event type at some position in the sequence, it may not be chosen elsewhere for distinguishing a 'B' at any other position. Also, if a format is used to distinguish an A (or B) event at one point in the sequence, it should be used at all points (different formats should not be chosen for the same event type at different positions in the sequence).

A Diversion: Non-Events

All format variations that do not contribute to navigating through the conceptual maze, i.e., which neither advance nor lock up the stronglink's UQS discriminator, are by definition "non-events". In abnormal environments, any number of non-events might be generated between actual stronglink events. However, such non-events could not cause the stronglink's UQS discriminator to advance and would not be assured[4] to cause the discriminator to lock up. Otherwise, they would be events, not non-events. Thus, any non-events that might occur would leave the stronglink's UQS discriminator unchanged and still capable of advancing

[4]Only those event types needed by the stronglink's discriminator to advance to its enabled condition can be assured to be discriminated in abnormal environments.

toward its enabled condition (or of locking up).

Such non-events cannot contribute to the safety of the UQS because, even if they are generated in an accident, they can play no part in determining whether or not the stronglink's UQS discriminator is advanced to its enabled condition before it is locked up.

Chapter Summary

The purpose of a UQS is to communicate the safety-critical intent to detonate a nuclear weapon from the information input source interface to a stronglink discriminator in the weapon in a manner that is highly unlikely to be duplicated or simulated in normal environments or in a broad range of ill-defined abnormal environments. If a UQS is properly implemented (using the features described in this report), the benefit is to minimize/eliminate the necessity for the UQS communication channel to be carefully designed, analyzed, tested, and controlled in production and use to assure predictability in abnormal environments.

Chapter II

THE ENGINEERING (ANALYSIS AND SYNTHESIS) OF PATTERNS FOR UNIQUE SIGNALS

Introduction

The previous chapter described the UQS as a sequence of events whose pattern must be carefully engineered to be highly unlikely to be duplicated or simulated in a broad range of normal and ill-defined abnormal environments. We now address the topic of that pattern and discuss how it can be engineered to meet its nuclear safety requirement.

A UQS is a sequence of two types of events. For convenience, the UQS event types are labeled alphabetically, e.g., an 'A' event type or a 'B' event type. The formats that distinguish the types of UQS events are not safety-critical and may be changed (translated) from point to point along the UQS communication channel, as long as it's done one event at a time with no dependence on event position in the sequence. All other formats are non-events and are not considered in engineering patterns for UQSs.[5] The order of the UQS events necessary to enable the stronglink is called the pattern of the UQS. Unlike the UQS event formats, the pattern of the UQS is safety-critical. This pattern must be engineered to be highly unlikely to be duplicated or simulated in a broad range of normal or ill-defined abnormal environments.

"Analysis" refers to evaluation of an existing pattern. "Synthesis" refers to creation of a new pattern suitable for use in a UQS. The two are based on the same considerations; most of the discussion that follows applies equally well to either.

The approach we will follow to develop desirable characteristics of a pattern of a UQS is to first examine some undesirable patterns and determine how to avoid the nuclear safety concerns associated with them. The basis for safety concerns, and therefore, the basis for developing the nuclear safety considerations to protect against those concerns, is scrutiny of natural phenomena and engineering experience with what can go wrong in the real world of abnormal environments. To be more specific, the primary phenomena are often observed to exhibit non-random behavior. Regularity, as well as randomness, is seen in abnormal environments; the two are often mixed in some fashion. Recognizing that malfunctioning equipment has the potential to act as an inadvertent generator only serves to increase one's expectation that some degree of regularity may appear in abnormal environments.

The structure of a UQS restricts the nuclear-safety impact of regularity in accident generators by sequencing in time the actions that would be required to generate the correct UQS. However, even with this restriction working in favor of abnormal-environment nuclear detonation safety, it is crucial that a pattern be employed in the UQS that is not susceptible to regularities in inadvertent generators. There are a

[5]Ignoring non-events reflects the behavior of the stronglink's UQS discriminator, which does not respond to non-events.

number of considerations in creating acceptable UQS patterns, and these are most effectively illustrated by first showing undesirable patterns and then the considerations necessary to reduce/eliminate the vulnerabilities.

An Undesirable Pattern

First, consider an undesirable pattern consisting of 23 'A' type events followed by one 'B' type event:

A A A A A A A A A A A A A A A A A A A A A A B

An inappropriate assumption would be that inadvertently generated events will be produced in an equally-likely manner. However, particularly in abnormal environments, this is not necessarily the case. That is, the likelihood that the next event will be an 'A' cannot be assumed to be the same as the likelihood that it will be a 'B'. The equally-likely assumption would be expressed mathematically as P(A) = P(B). Furthermore, since mathematically the sum of the probabilities of all outcomes must equal one, and the only possible outcomes are 'A' and 'B', the equally-likely assumption leads to:

$$P(A) = P(B) = 1/2$$

If the equally-likely assumption (and independence) were true, the probability that the pattern of 23 'A's and 1 'B' would be generated in abnormal environments could be calculated by the product of the probabilities[6] of each event as follows:

$$P = \left(\frac{1}{2}\right)^{23} \times \left(\frac{1}{2}\right)^{1} = \left(\frac{1}{2}\right)^{24} = 0.6 \times 10^{-7}$$

But, what if 'A's happened to be generated more often than 'B's in some abnormal environment? Specifically, consider the case where the probability of an 'A' is 23/24:

$$P(A) = 23/24 \text{ and } P(B) = 1/24$$

[6]Note that multiplying probabilities is permissible mathematically only if the probabilities are independent.

Then, the probability that the pattern of 23 'A's and 1 'B' would be generated by independent selections in abnormal environments would be calculated as:

$$P = \left(\frac{23}{24}\right)^{23} \times \left(\frac{1}{24}\right)^{1} = 0.2 \times 10^{-1}$$

This dramatic change in the calculated probability that the pattern would be generated serves as a motivation to take a closer look at the range of probabilities of generating an 'A' -- and of a 'B' -- that could occur in abnormal environments.

Range of Probabilities of an 'A'

In probabilistic modeling of gambling games (customarily occupying a prominent place in probability and statistics texts) an equally-likely assumption is standard. However, in the real world of abnormal environments, there is no reason to assume that 'A's and 'B's will be generated in equal numbers.

In fact, there are no physical constraints on the values that P(A) and P(B) may take in abnormal environments. The only constraints are that every probability must lie in the range from zero to one, and the sum of the probabilities of all possible outcomes must equal one.

$$0 \leq P(A) \leq 1 \text{ and } 0 \leq P(B) \leq 1$$

$$P(A) + P(B) = 1$$

Figure II-1 illustrates these relationships in graphical form. The range of P(A) is plotted on the abscissa, and the range of P(B) on the ordinate. The diagonal line represents the constraint that the sum of the two probabilities equal one. Thus, the probabilities actually found in an accident may lie at <u>any</u> point on the diagonal line. The point marked at the center of the plot is for the equally-likely case, merely one of the infinite number of points on the line. While the equally-likely point might occur in abnormal environments, any other point on the line also might occur -- including the point marked in the lower right-hand corner which corresponds to the set of probabilities that generated the extremely high calculated probability of independent-event pattern generation in the previous section.

Evaluation of a Pattern Over the Range of Probabilities

A pattern that is a candidate for use in a UQS must be evaluated over the full range of P(A)s and P(B)s shown in Figure II-1.

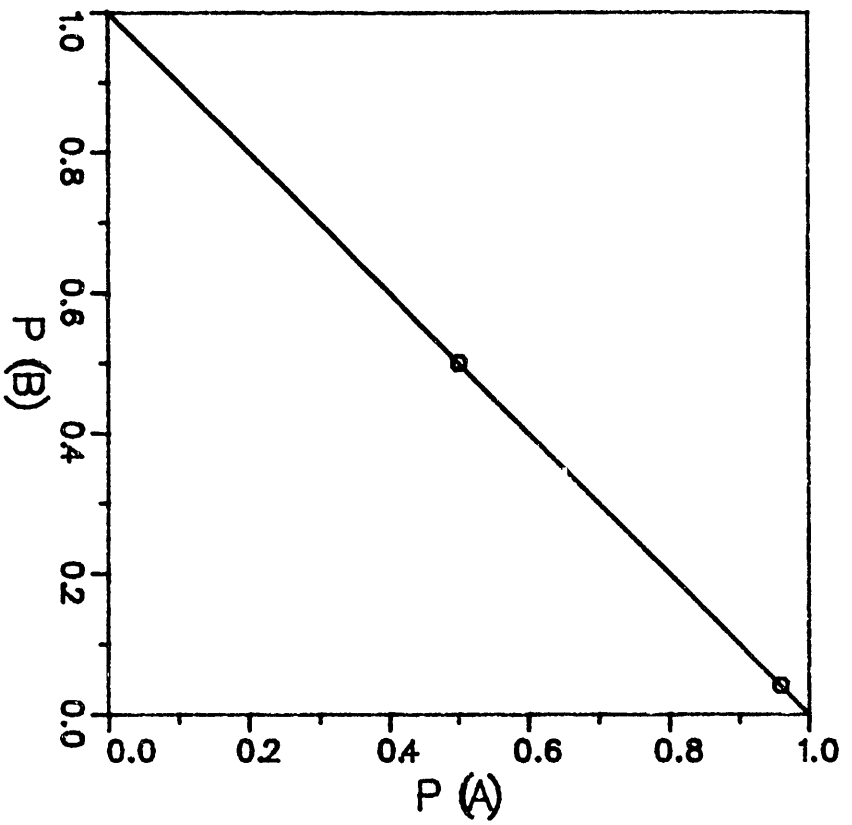


Figure II–1
Range of Potential Accident Threats
P(A) and P(B)

Since P(A) and P(B) are related by the constraint that their sum equals one, we will vary P(A), and P(B) will be determined by the value of P(A). Thus, candidate patterns for UQSs must be evaluated over the entire range of P(A).

For any pattern, a plot could be prepared showing the calculated probability of its independent-event generation as a function of P(A). The calculation for each point on the plot would be similar to the calculations shown earlier in this chapter. Such a plot for the pattern of 23 'A's and 1 'B' is shown in Figure II-2.

The dashed lines on Figure II-2 mark the two probabilities calculated previously and illustrate vividly that the maximum value of the curve (least safe point) does not necessarily coincide with equally-likely probabilities. In fact, the maximum value occurs at the point where P(A) and P(B) are in the same ratio as the ratio of 'A's and 'B's in the pattern, a result which is intuitively satisfying[7] as well as being mathematically demonstrable.

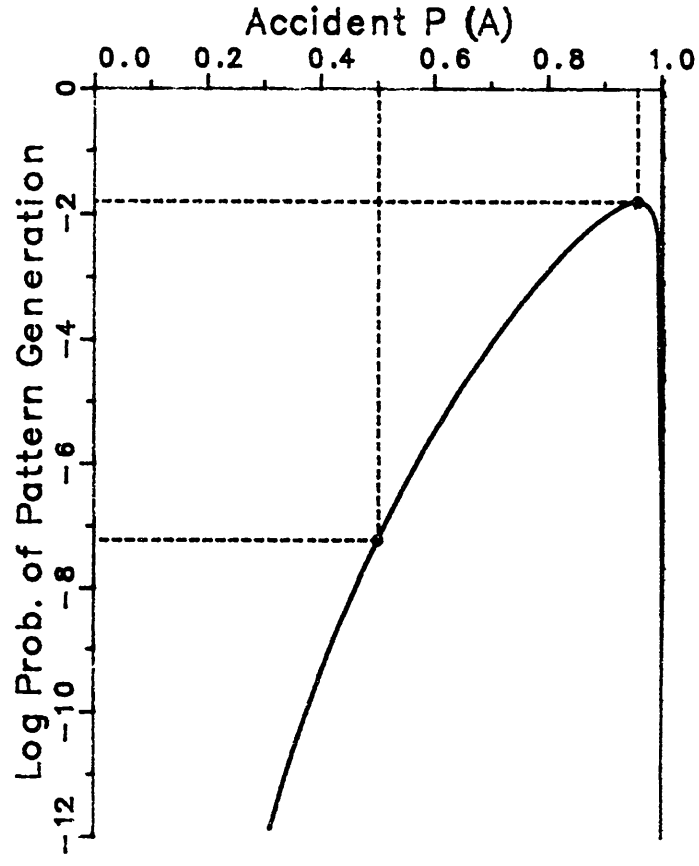
Nuclear safety requirements must be met in <u>all</u> credible abnormal environments. Any P(A) on the top axis of Figure II-2 could occur in abnormal environments, with its corresponding calculated probability of pattern generation. Therefore, the level of safety assured in all abnormal environments is represented by the maximum value of the curve. It should be stressed that the use of the maximum value to evaluate a pattern does not imply a belief that every accident will be that bad. Rather it recognizes that an accident <u>could</u> be that bad and safety must be assured under those conditions.

<u>Event-Wise Balance</u>

Now, consider a <u>desirable</u> pattern with equal numbers of 'A's and 'B's:

A B A A A A B A A B A A B B B B A B B B B A A B

[7]It should be noted that, while this result does follow intuition, such is not always the case in nuclear safety.



Event Counts

A = 23 B = 1

Figure II-2

Probability of Independent-Event Generation for a Range of Accident Threats for the Pattern:

A A A A A A A A A A A A A A A A A A A A A A B

Figure II-3 replaces the skewed plot of Figure II-2. Now, the maximum value of the curve occurs at the equally-likely point. This means that, for a pattern with equal numbers of 'A's and 'B's, the worst P(A) that can happen in an abnormal environment is 1/2 (equally-likely generation of 'A's and 'B's). Any other (skewed) P(A), P(B) set would result in a decreased calculated probability of generating this pattern. A pattern with equal numbers of 'A' and 'B' type events is termed "event-wise balanced".

Thus, we have developed one consideration for a pattern of a UQS:

***** The pattern should be event-wise balanced (or as equal as possible), i. e., it should have equal numbers of 'A' type events and 'B' type events.**

Another Undesirable Pattern

Event-wise balance is not enough to assure safety in a wide range of abnormal environments.[8]

Consider the following undesirable event-wise balanced pattern:

A B A B A B A B A B A B A B A B A B A B A B

Periodic patterns are not uncommon in normal environments. It is not hard to imagine how a tendency toward alternating might arise in abnormal environments. For instance, an energized wire might swing between two other wires, one connected to generate an 'A' event, the other a 'B'. The pattern displays extreme susceptibility. The basic problem is that uncertainty (dissimilarity to the ordinary) is lacking. Patterns lacking uncertainty do not meet UQS requirements.

Range of Conditional Probabilities

By including the first-order conditional probabilities, the number of variables is raised from two to six. As was the case for the independent probabilities alone, the values each one may take in abnormal environments can lie anywhere in the range from zero to one. Thus, we have:

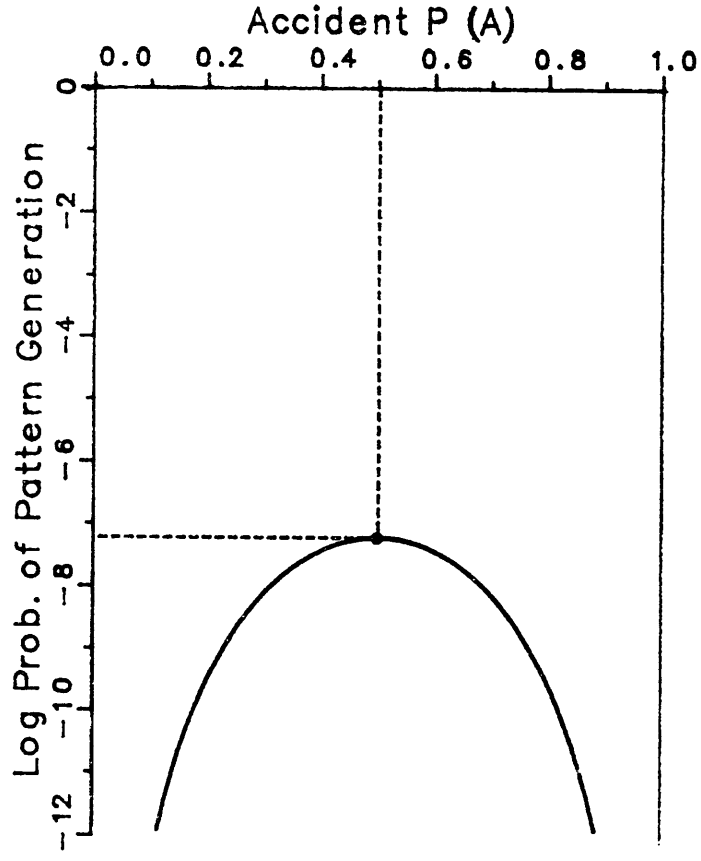
$$0 \leq P(A) \leq 1 \quad \text{and} \quad 0 \leq P(B) \leq 1$$

$$0 \leq P(A|A) \leq 1 \quad \text{and} \quad 0 \leq P(B|A) \leq 1$$

$$0 \leq P(A|B) \leq 1 \quad \text{and} \quad 0 \leq P(B|B) \leq 1$$

Any accident probabilities must fall within bounds. Specifically, the sum of the probabilities of all outcomes from each condition must equal

[8]Necessary but not sufficient.



Event Counts

A = 12 B = 12

Figure II-3

Probability of Independent-Event Generation for a Range of Accident Threats for the Pattern:

A B A A A A B A A B A A B B B B A B B B B A A B

one. Furthermore, conditional probabilities and the associated unconditional ones are constrained. We thus have four constraint equations:

$$P(A) + P(B) = 1$$

$$P(A|A) + P(B|A) = 1$$

$$P(A|B) + P(B|B) = 1$$

$$P(A) = P(A|A) \times P(A) + P(A|B) \times P(B)$$ [9]

Figure II-4 illustrates these relationships in graphical form. This plot is analogous to Figure II-1. However, due to the number of variables, a three-dimensional plot is necessary. The ranges of P(A) and P(B) are plotted on the vertical axis in opposite directions so that they sum to one everywhere along the axis. The ranges of P(A|A) and P(B|A) are plotted on the lower left-hand axis, also in opposite directions. Likewise, P(A|B) and P(B|B) on the lower right-hand axis.

The curved surface meets the four above constraints. Therefore, the probabilities actually found in an accident may lie in <u>any</u> point on this surface. The point marked at the center of the plot is for the equally-likely case (all probabilities equal 1/2), merely one of the infinite number of points on the surface. While the equally-likely point might occur in abnormal environments, any other point on the surface also might occur -- including the point marked on the right-hand edge which corresponds to the set of probabilities that generates the maximum value on the next figure.

<u>Evaluation of a Pattern Over the Range of Conditional Probabilities</u>

In a fashion analogous to the unconditional probability case shown in Figure II-1, a pattern that is candidate for use in a UQS must be evaluated over the full range of probabilities defined by the curved surface in Figure II-4.

Six probability variables combined with four constraint equations result in two unconstrained variables.[10] There is considerable freedom in selecting which two probabilities to use as unconstrained variables. For this analysis, P(A) and P(A|A) have been chosen. Any pair of values for these two probabilities represents a point on the curved surface of Figure II-4; and, any point on that curved surface is represented by such a pair of values. In order to account for the full range of potential conditions (and therefore avoid a catastrophic vulnerability), candidate patterns for

[9] From symmetry, one might correctly expect that there is a fifth equation: $P(B) = P(B|A) \times P(A) + P(B|B) \times P(B)$. However, it can be derived from the other four, and thus, is not necessary.

[10] The other four probabilities can be calculated from the unconstrained pair of probabilities and the constraint equations.

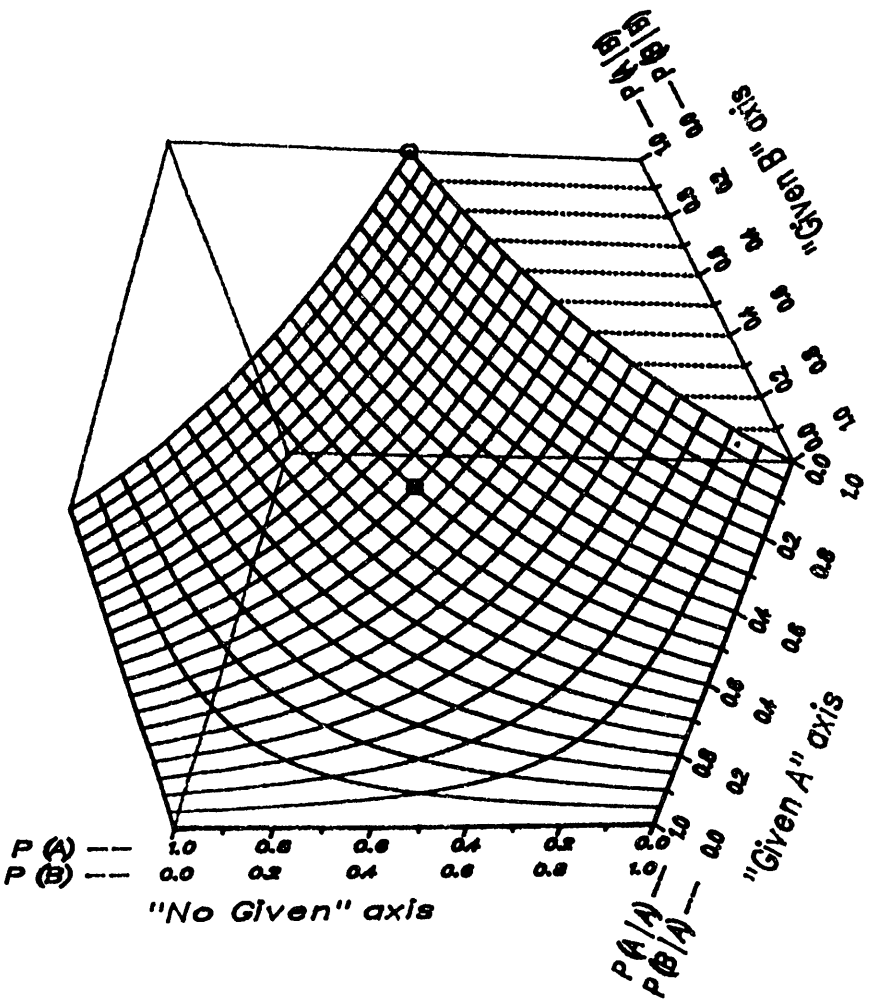


Figure II–4
Range of Potential Accident Threats
P(A), P(B) and P(A|A), P(B|A) and P(A|B), P(B|B)

UQSs must be evaluated over the entire range of P(A) and simultaneously the entire range of P(A|A), which covers the entire surface of Figure II-4.

For any pattern, a plot could be prepared showing the calculated probability of generation as a joint function of P(A) and P(A|A) similar to Figure II-2 for the unconditional probability case.

Because there are two unconstrained variables, a three-dimensional plot is required. Figure II-5 is such a plot for the pattern of alternating 'A's and 'B's discussed earlier. P(A) and P(A|A) are the two axes on the top plane. There is a one-to-one relationship between the points on this plane and the curved surface in Figure II-4. Thus, every point on the top plane represents a set of conditional probabilities that could occur in some abnormal environment. Each point on the curved surface is at the calculated probability of pattern generation for the point directly above it on the top plane.

The dashed lines on Figure II-5 mark the calculated probability for an inappropriate equally-likely assumption. However, the maximum value of the curved surface is at the upper-right edge of the top plane at the point where P(A) = 1/2 and P(A|A) = 0. As was the case for unconditional probabilities in Figure II-2, this point matches the rates of occurrence in the pattern, i.e., 'A' events occur 1/2 the time and 'A' never follows 'A' in the pattern of alternating 'A's and 'B's.

In this example, the maximum value of the calculated probability of pattern generation is 1.0. This reflects the total absence of uncertainty in the alternating pattern.

Pair-Wise Balance

The pattern used as a desirable example in the previous discussion of unconditional probabilities leading to the event-wise balance consideration was:

A B A A A A B A A B A A B B B B A B B B B A A B

This pattern is "pair-wise" balanced as well as event-wise balanced. Tabulating the number of times each type of event is followed by each type of event:

		Following Event A	Following Event B
Leading Event	A	6	6
	B	5	6

These counts of event pairs are equal except for a missing 'B A' pair. There is one less pair than the number of events in the pattern because the last event in the pattern has no event following it to form the 24th pair.

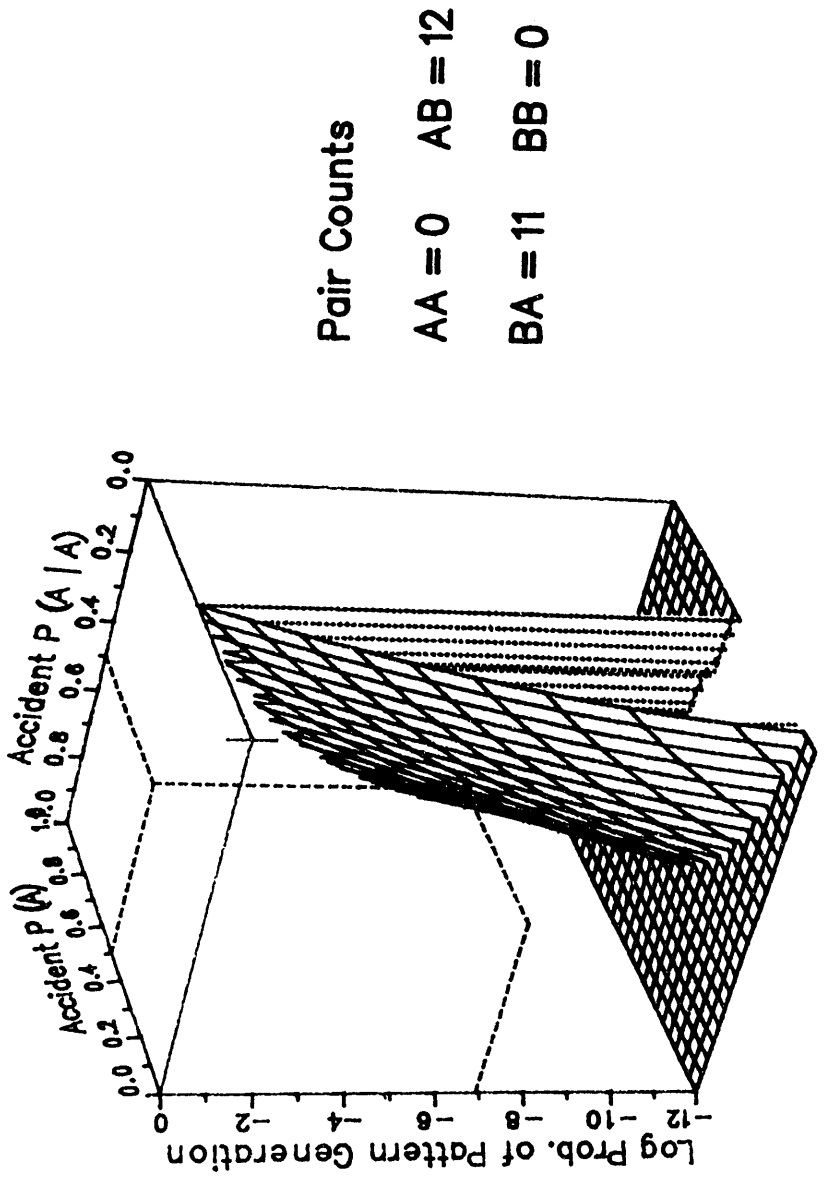


Figure II-5

Probability of First-Order-Dependence Event Generation for a Range of Accident Threats for the Pattern:

A B A B A B A B A B A B A B A B A B A B

For this pair-wise balanced pattern, Figure II-6 replaces the skewed plot of Figure II-5. Now, the maximum value of the curved surface occurs nearly at the equally-likely point. The reason that the maximum value is not exactly at the equally-likely point is that the missing event pair prevents the pattern from being perfectly balanced.

Therefore, a second consideration for a pattern of a UQS to accompany event-wise balance is that the pattern should also be pair-wise balanced, i.e., it should have equal (or as equal as possible) numbers of 'A A' and 'A B' event pairs and should have equal (or as equal as possible) numbers of 'B A' and 'B B' event pairs. For an event-wise balanced pattern, the number of event pairs beginning with an 'A' event is as equal as possible to the number of event pairs beginning with a 'B' event. Pair-wise balance can then be defined by the simpler and more convenient statement that:

*** **The pattern should have equal (or as equal as possible) numbers of 'A A', 'A B', 'B A', and 'B B' event pairs.**

A Formula for Calculating the Maximum Value for the First-Order Conditional Probability Case

As one means of evaluating a potential pattern of a UQS, it is sometimes useful to compute the maximum value of the calculated probability that the pattern will be generated for the first-order conditional probability case. A formula can be developed that minimizes the needed computation. The first step in using conditional probabilities to evaluate a pattern is to count "event pairs", that is, the number of times an 'A' event is followed by another 'A' event, an 'A' by a 'B', a 'B' by an 'A', and a 'B' by a 'B'. Let AA = the number of 'A A' event pairs, AB = the number of 'A B' pairs, etc. Note that the letters are in the reverse order of that in the conditional probability notation, i.e., P(B|A) refers to 'A B' event pairs.

Taking the previous example pattern:

A B A A A A B A A B A A B B B B A B B B B A A B

We find:

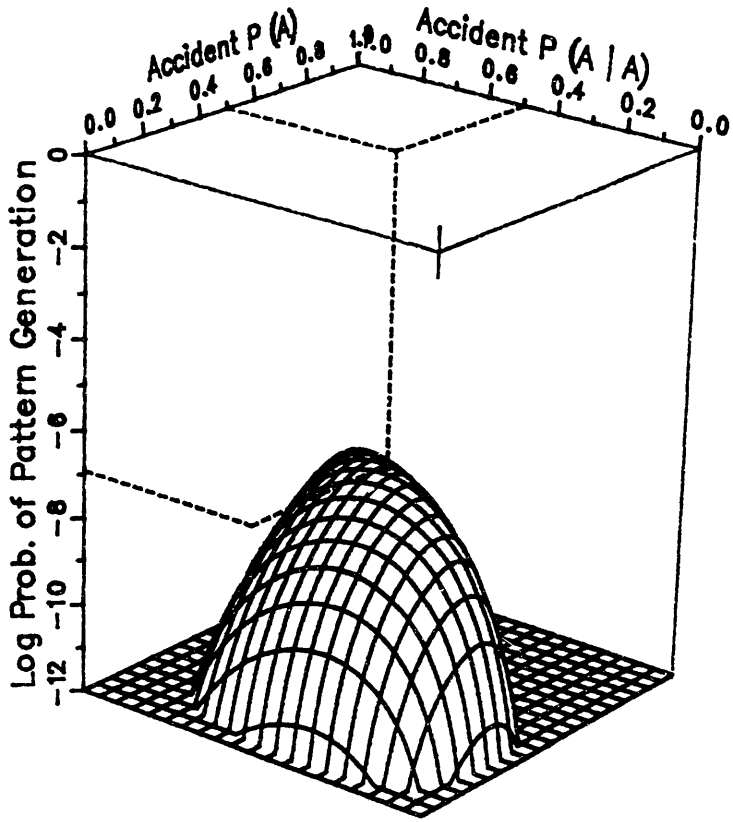
$$AA = 6;\ AB = 6 \quad \text{and} \quad BA = 5;\ BB = 6$$

Note that each event is a member of two event pairs, except for the end events. Also note that, because of the end events, there is one less event pair than there are events.

The formula for calculating the first-order conditional probability of generation of the pattern can now be written:

$$P = P(A|A)^{AA} \times P(B|A)^{AB} \times P(A|B)^{BA} \times P(B|B)^{BB}$$ [11]

[11] One could consider a separate probability for the first event in the sequence. The difference (a factor of two for a balanced pattern) is insignificant.



Pair Counts

AA = 6 AB = 6

BA = 5 BB = 6

Figure II-6
Probability of First-Order-Dependence Event Generation for a Range of Accident Threats for the Pattern:
A B A A A A B A A B A A B B B B A B B B B A A B

Note: $P^0 = 1$ for all values of P including 0

The maximum value of the first-order conditional probability of pattern generation occurs at the point where the conditional probabilities are in the same ratio as the ratio of event pairs for the condition. That is:

$$P(A|A) = \frac{AA}{AA+AB} \; ; \; P(B|A) = \frac{AB}{AA+AB}$$

$$\text{and } P(A|B) = \frac{BA}{BA+BB} \; ; \; P(B|B) = \frac{BB}{BA+BB}$$

Substituting these ratios for the conditional probabilities in the previous equation gives:

$$P_{calc} = \left\{\frac{AA}{AA+AB}\right\}^{AA} \cdot \left\{\frac{AB}{AA+AB}\right\}^{AB} \times \left\{\frac{BA}{BA+BB}\right\}^{BA} \times \left\{\frac{BB}{BA+BB}\right\}^{BB}$$

Combining like factors in the denominator yields the final, computational form:

$$P_{calc} = \frac{AA^{AA} \times AB^{AB} \times BA^{BA} \times BB^{BB}}{(AA+AB)^{(AA+AB)} \times (BA+BB)^{(BA+BB)}}$$

This theoretical calculation is limited to first-order conditional probabilities, but it is a useful metric for comparing patterns. Note that higher order and other conditional probabilities represent potential threats that can increase P_{calc}. Although these threats must be recognized in analysis, they are not directly included in synthesizing UQS patterns, because the capability of pattern design to defeat conditional probability threats diminishes rapidly with increases in threat complexity. For these reasons, P_{calc} should not be considered an absolute measure of actual probabilities. Actual threats may be greater (see subsequent section on "Number of Events Required in a Pattern for a Single-Try UQS"), even when events are communicated ideally (See Chapter III).

More Numerical Nuclear Safety Considerations for Patterns for UQSs

In addition to the event-wise and pair-wise balance considerations that have been presented, other numerical nuclear safety considerations have also been developed for patterns for UQSs. Although numerical in nature, these additional safety considerations do not rely on the level of mathematical "proof" employed for balancing.

The fundamental bases for nuclear safety considerations for patterns for UQSs is engineering, in addition to mathematics. That is, nuclear safety is based on observation and study of the way things tend to happen in the real world. In the case of balancing, mathematics could be exclusively applied. Such is not the case for the safety considerations in the remainder of this chapter.

Consider the following undesirable pattern, which is both event-wise and pair-wise balanced:

A B B A A B B A A B B A A B B A A B B A A B B A

This pattern lacks uncertainty because of its inherent periodicity, and it therefore is vulnerable to being generated in abnormal environments. The mathematical treatment leading to event-wise and pair-wise balancing addressed situations in which events were generated by a process that, at most, retains an effect from only the previously generated event. Because of its mathematical basis, the balancing discussed previously provides high confidence that any event-wise and pair-wise balanced pattern will have a bounded response to accident generators that do not retain any effect from events before the immediately preceding one. This balancing provides no protection against any form of inadvertent generation that does retain effects from more than one event back.

One engineering concern that leads to a safety consideration is the observation that, in nature, processes tend to continue once begun. Specifically, a pattern of a UQS should not be susceptible to inputs with long strings of 'A' or 'B' type events together. The consideration that is applied to patterns is that no continuous string of events of the same type should be longer than four events. A four-event limit is achievable, while attempting to set a limit at three would severely undercut the capability of meeting the other considerations for a pattern.

Engineering experience also leads to the observation that natural processes often tend to be regular, or at least tend to exhibit some degree of regularity. To provide some protection against regularity in an accident generator, a safety consideration has been developed that the numbers of "groupings" of 'A' and 'B' event types should be different. The word "groupings" is used here to refer generically to a specific-length string of events of like type, e.g., a single event, a pair of like events, a triple, etc. As applied, this consideration means that the number of 'A' type events appearing alone should be different from the number of single 'B' events, the number of pairs of 'A's should be different from the number of 'B' pairs, etc. The intention is to require an accident generator to generate 'A' type events "differently" from the way it generates 'B' type events.

A further safety consideration to protect against regularity in an inadvertent generator is to minimize the maximum length of repeated strings of events. The purpose is to prevent an accident which has correctly generated part of the pattern by chance from generating more of the pattern by merely repeating the process. These forms of regularities are limited to strings of about six events.

Minimizing the maximum length of repeated strings of events in a pattern can be extended to include a check against strings and their complements, where "complement" means that 'A' type events have been replaced with 'B' type events, and 'B's with 'A's. A further extension is to check strings against strings in reverse order. Finally, strings are checked against complemented strings in reverse order.

Non-Numerical Nuclear Safety Considerations for Patterns for UQSs

In addition to the numerical considerations for UQS patterns discussed above, non-numerical considerations have also been developed. As is the case for the numerical considerations, the basis for developing these non-numerical considerations is engineering experience.

The first of these non-numerical nuclear safety considerations is that the pattern be non-periodic. The numerical considerations discussed previously help eliminate periodicities. However, they do not comprise a complete screen. As an example, consider the following pattern:

A A B B B A A A B A B A A A B B B A B A B B B A

This pattern is basically periodic (3 'A's, 3 'B's, etc.) with only two breaks in its repeating pattern. The two underlined events are complemented from a periodic pattern. Such patterns can pass the previously developed numerical safety considerations, all of which are met by this pattern. Therefore, a pattern of a UQS must be examined for periodicities that escape the numerical safety considerations.

Similarly, a pattern of a UQS is examined to ensure that it is non-symmetrical end-to-end. Again, the previously discussed numerical safety considerations will eliminate many patterns that are symmetrical. However, a non-numerical check is still used to catch any that pass the numerical considerations.

An Additional Safety Consideration for Multiple UQSs

Up to this point, all of the nuclear safety considerations that have been developed for a pattern of a UQS apply to a single pattern in isolation. The modern approach to nuclear detonation safety calls for the use of two, independent, abnormal-environment safety subsystems in each nuclear weapon design in order to meet the stringent abnormal-environment nuclear safety requirements imposed. These two abnormal-environment safety subsystems must be independent for common failure modes to be avoided. Common-mode failures can arise in many different ways. While there are important implications for safety subsystem hardware, the common-mode failure of concern in this chapter on patterns for UQSs is the potential that the operating signal for one safety subsystem might affect the likelihood that the signal for the other subsystem could be inadvertently generated in abnormal environments.

The most obvious way for such a common-mode failure to occur would be for the designer of a nuclear weapon to use the same operating signal for both safety subsystems. If this were done and the signal for one subsystem were inadvertently generated by any means, one undesired connection in an abnormal environment could send the operating signal to the other safety subsystem and defeat it as well.

Only the pattern of a UQS is safety-critical. The formats of the individual events are not safety-critical and may be translated from one form to another at any point in the UQS communication channel. Thus, for

the case in which the two operating signals are both UQSs, if their patterns were identical (even though the event formats were different), one UQS could be translated into the other in an abnormal environment merely by translating event formats. Therefore, inadvertent generation of the pattern of one UQS in an abnormal environment would constitute generation of the common pattern of both UQSs, an obvious common-mode failure.

More subtly, even if the patterns of the two UQSs are not identical, the potential exists for a pair of patterns to be selected such that the presence of one pattern could afford an accident greater likelihood of generating the other pattern. Such would be the case if the two patterns had substantial portions in common. Duplicate strings would be an even greater susceptibility if they were aligned between the two patterns.

In order to maintain the required independence, patterns for the UQSs in the two safety subsystems in a nuclear weapon design should have duplicate strings of minimum length. Further, particular attention should be paid to duplicate strings that are aligned between the two patterns. For these checks, complements (changing 'A's to 'B's, and 'B's to 'A's) should be treated the same as the original patterns because the 'A' format of one UQS could easily be (or be translated to) the 'B' format of the other.

An Extension of the Safety Consideration for Multiple UQSs

In practice, each pattern of a UQS is associated with the hardware UQS discriminator and stronglink it enables. Usually, several different nuclear weapon designs use the same stronglink, or similar ones using the same pattern. Therefore, the patterns for the UQSs of different weapon designs are used for the same purpose, because they might be on board a common carrier (e.g., ship or aircraft). That is, a pattern used for intent in one design (and thus provided before launch or release) would not be used for trajectory in another weapon design.

Application of the Safety Considerations for Patterns

Computer programs are used to calculate the values of the numerical nuclear safety considerations and most (if not all) of the non-numeric considerations. Such programs sort through all potential patterns, winnowing out all but those (hundreds) that meet the numerical considerations and all but a few (tens) of the remainder.

Number of Events Required in a Pattern for a Single-Try UQS

One of the most fundamental and important characteristics of a pattern of a UQS is simply how long it is.

In meeting modern nuclear detonation safety requirements, the objective for each independent safety subsystem is that the probability of the subsystem failing to perform its safety function must be less than 10^{-3} to 10^{-4} in all normal environments and in all credible combinations of abnormal environments. (This decision was made during the formative period of the abnormal-environment safety approach to assure that the system requirement of less than 10^{-6} could be met.) The subsystem requirement applies to the

combination of all abnormal environment failure modes of the entire safety subsystem. The likelihood of inadvertent generation of the pattern of the UQS in abnormal environments should be insignificant compared to the likelihood that hardware engineered features (safety devices) will fail to isolate energy in abnormal environments. This assures that the UQS, if properly implemented, will not be a critical concern.

A number of nuclear safety considerations for patterns for UQSs have been presented in this chapter. Only the first two (event-wise and pair-wise balance) are incorporated in the computational formula for a calculated first-order conditional probability of inadvertent pattern generation. That formula omits most of the safety considerations presented -- and the safety concerns behind them. In determining how long a pattern of a UQS should be, allowance must also be made for subtle, unrecognized susceptibilities in the pattern, which may cause the effective length to be reduced. Therefore, the pattern can tolerate two to three orders of magnitude reduction in safety.

As a result of the above factors, a length of 24 events has been established for patterns for UQSs for single-try stronglinks.[12] This number is not entirely based on probability calculations. It also represents engineering judgment taking into account all the safety considerations for patterns discussed in this chapter as well as providing margins for unrecognized pattern susceptibilities and potential hardware problems. It has proven prudent and adequate.

Number of Events Required in a Pattern for a Multiple-Try UQS

There are additional safety concerns with multiple-try (reset and re-try a possibly different pattern) UQS discriminators. In the interest of completeness, the nuclear safety considerations involved in selecting the length of a pattern for a multiple-try UQS are discussed in this section.

The difference between multiple-try and single-try UQS discriminators is that a multiple-try discriminator responds to a third UQS event type as well as the two that have been involved in the descriptions to this point. On receipt of this "Reset" type event, a multiple-try UQS discriminator resets itself directly to its initial, safe condition -- even if it had been locked up by an event in an incorrect pattern. The multiple-try discriminator is then capable of responding to further event inputs, hence its designation as "multiple-try".

The safety theme for multiple-try UQS discriminators can only be delay, not prevention. Therefore, for a multiple-try UQS (unlike the single-try case), it is not enough that one inadvertent attempt be highly unlikely to generate the correct pattern. For the delay safety theme to be effective, it must be highly unlikely that any one of a long series of repeated tries will generate the correct pattern.

[12]Differences to nuclear safety between single-try and multiple-try stronglinks are discussed subsequently.

One's first impression might be that inadvertent generation of the correct pattern in the midst of a series of incorrect patterns would not be catastrophic on the grounds that the next (incorrect) pattern would "undo" the unsafe results of the correct one. However, there is no assurance in abnormal environments that enabling the stronglink could not cause a change in logic that would cut off further input to the UQS discriminator. In fact, similar logic has been incorporated for reliability purposes.

For a multiple-try UQS, the "unlikelihood" that the correct pattern will be generated per try should be better than the unlikelihood of a single-try UQS by a factor of the largest credible number of tries in all abnormal environments. This condition is necessary in order for the multiple-try UQS to provide a level of abnormal-environment safety commensurate with that of a single-try UQS. In probability terms:

$$P(\text{UQS generation}) = P(\text{per try}) \times N_{tries}$$ [13]

Thus, the requirement for the per-try probability is:

$$P(\text{per try}) = \frac{P(\text{UQS generation})}{N_{tries}}$$

A single-try UQS discriminator has the important fundamental advantage of restricting the value of N_{tries} to one. However, certain types of delivery system requirements for the option of reversibility after commitment led to a multiple-try discriminator. For a multiple-try UQS, the potential number of tries is equal to the time an abnormal environment (e.g., electrical faults) could exist uncorrected (which includes the time it might go undetected), times the number of tries per unit time (or, equivalently, divided by the time required for each try). As an equation:

$$N_{tries} = \frac{t_{\text{abnormal environment}}}{t_{\text{per try}}}$$

A time of 30 days was selected as $t_{\text{abnormal environment}}$, since this would assure that if an electrical fault[14] were present at the time of weapon loading, and if the fault caused the switch to be operated as rapidly as possible, the likelihood of completing the switch operation would be suitably remote. These very safety-conservative assumptions would assure that no operational restrictions were necessary to implement the unique signal concept.

---

[13] Although this formula is, strictly speaking, an approximation, it is an excellent one in the range of very small probabilities for nuclear detonation safety.

[14] This is one of many cases where the most severe abnormal environment is not necessarily a "worst case" system catastrophe or failure.

The last nuclear safety consideration involved in selecting the length of a pattern for a multiple-try UQS is $t_{per\ try}$. We must first determine what constitutes a try; there are two different cases, depending on which of two different assumptions are made concerning how "Reset" type events are generated. The two different assumptions are: 1) "Reset" type events are generated randomly along with 'A' and 'B' type events in an endless string; and 2) "Reset" type events are generated at correct positions in the endless string.

If "Reset" type events are assumed to be generated randomly along with 'A' and 'B' type events in an endless string, each new event in the string must be considered the end of a new try because the stronglink could change from a not-enabled condition to an enabled condition after any new event. However, if "Reset" type events are assumed to be generated at correct positions in the endless string, a new try would occur only on the event immediately preceding a "Reset" event.

The increased rate of tries under the first assumption is counterbalanced by the possibility of a "Reset" type event being generated prematurely and terminating a sequence of 'A' and 'B' type events that was the correct pattern of the UQS up to that point. Calculating a probability of generation of the correct pattern (including a leading "Reset" type event) differs from the calculations shown previously in this chapter because of the added event type. However, calculations made using the first assumption approximate those using the second assumption; the calculation for the second assumption follows the formula derived earlier.

The result is that $t_{per\ try}$ is the shortest credible time for the stronglink's UQS discriminator to accept the complete pattern of the UQS including a leading "Reset" type event. As a corollary, probabilities (e.g., P_{calc}) are calculated using the previously derived formula for 'A' and 'B' type events without regard to the "Reset" type event.

To meet a required level of unlikelihood of inadvertent UQS generation, the unlikelihood per try must be:

$$P(\text{per try}) = P(\text{UQS generation}) \times \frac{t_{per\ try}}{t_{abnormal\ environment}}$$

Summary of Nuclear Safety Considerations for Patterns for UQSs

The pattern of the UQS for a stronglink safety device must be carefully engineered to assure that it is highly unlikely to be generated in a broad range of ill-defined abnormal environments. In order to meet this nuclear detonation safety goal, a number of safety considerations have been developed in this chapter. These nuclear safety considerations for patterns for UQSs include:

- A sufficient number of events: 24 for a single-try (not remotely resettable) device, and many more for a multiple-try (remotely resettable) device (47 were used in the MC2969, but this number is device-dependent and application-dependent).
- Event-wise balanced (as nearly as possible equal numbers of 'A' type events and 'B' type events).
- Pair-wise balanced (as nearly as possible equal numbers of 'A A', 'A B', 'B A', and 'B B' pairs).
- No more than four 'A's or 'B's together.
- Different numbers of groupings (singles, pairs, etc.) of 'A's and 'B's.
- Minimal length of repeated strings, including complements and reverse order.
- Non-periodic.
- Non-symmetrical.
- Minimum length of strings repeated in all other patterns used for UQSs, with particular attention to strings aligned in the same position.

It is crucial to recognize that the development of these nuclear safety considerations for patterns for UQSs has been based on an implementation in which -- in a broad range of ill-defined abnormal environments -- each UQS event must be generated individually in the order of the engineered pattern. Therefore, in order for the safety benefits of a UQS to be realized, the UQS must be communicated as a sequence of unrelated (independent) events from the human/machine interface to the UQS discriminator in the stronglink safety device.

A Non-Unique Signal for Test and Training

It is desirable in some weapon systems to communicate a signal with characteristics similar to those of a UQS through the UQS communication channel on a more-or-less routine basis. Example purposes are crew training, reliability testing of the UQS communication channel, etc. Typically, live nuclear weapons either will not have been loaded or will have been isolated.

Examples of safety concerns are that a correct unique signal applied for test purposes may reach an unintended destination through faulty electrical insulation or faulty logic isolation. Unforeseen capture and storage of communications is possible in a complex weapon system, such that a test or training signal would still be available in the system when the live nuclear weapon was connected.

A real UQS can therefore not be used for routine test or training.[15] What is needed is a test and training signal that shares as many characteristics as possible with the real UQS yet does not compromise nuclear safety by undermining the UQS.

The structure of a UQS, that is, a sequence of unrelated events, is not safety-critical. Neither are the formats that define the types of UQS events. A test and training signal may be a sequence of events using the event formats of a real UQS, but with a different, non-uncertain pattern.

The entire discussion of this chapter prior to this section has been directed toward establishing considerations for uniqueness of a pattern of a UQS. We now reverse the process and present a non-uncertain pattern that violates the uniqueness considerations. This non-uncertain pattern is:

A B B A B B A B B A B B A B B A B B A B B A B B

This pattern is not balanced, either event-wise or pair-wise. It is periodic and not at all random-appearing. Therefore, it can be used for a test or training pattern without undermining any real UQS that is now in use or that may be synthesized at some future time.[16]

An additional test, useful for both reliability and safety, would be verification that each event in the sequence can actually be communicated as either an 'A' type event or a 'B' type event. This can be checked by a second test pattern that is the complement of the first:

B A A B A A B A A B A A B A A B A A B A A B A A

This pattern could be used immediately following the first, or it could be used at some other point in a test sequence. If two tests were to be incorporated for other reasons (presumably at different points in a test sequence), the second (complement) test pattern could be used for the second test.

---

[15] If a real UQS were to be used in a factory test, extreme care would have to be exercised to ensure that all traces are erased following the test.

[16] A similar pattern, ABBBBBABBBBBABBBBBABBBBB, has been incorporated in some designed systems. Its characteristics are similar to the pattern recommended here.

Chapter III

SAFETY CONSIDERATIONS FOR THE UQS COMMUNICATION CHANNEL

Payoff of Unique Signal Approach

An extremely important payoff of the UQS approach to nuclear detonation safety in abnormal environments applies to the UQS communication channel. By definition, the UQS communication channel includes all portions of a safety subsystem between the operator's UQS information source input device (see Figure III-1) and the weapon stronglink, including a potential range of devices from simple copper wires up through computer processors. In short, the properly implemented UQS concept allows nuclear safety in abnormal environments to be achieved at the level of the weapon system without requiring that the UQS communication channel be carefully designed, analyzed, tested, and controlled to be predictable in a broad range of ill-defined abnormal environments.

However, this payoff does not completely remove the UQS communication channel from all nuclear safety concern. The UQS communication channel must still be utilized in a way that does not undermine the UQS concepts developed in Chapters I and II.

Deriving Nuclear Safety Considerations for Utilizing the UQS Communication Channel

The nuclear detonation safety considerations for utilizing the UQS communication channel derive from the UQS concepts in Chapters I and II, and from the basic concept of a communication channel as a "passthrough" system (transmits information completely through the channel as received, with no information combination/processing).

A UQS is a sequence of unrelated and unrelatable events. In order to take advantage of independence, each UQS event is to be separate from and unrelated to the other UQS events in the sequence. This leads directly to the first nuclear safety consideration for utilizing the UQS communication channel:

*** **Each UQS event must be communicated individually.**[17]

The reasons behind this nuclear safety consideration (and the definition of a UQS event from which the consideration is derived) are apparent in Chapter II, which discusses how the pattern of a sequence of UQS events can be engineered to be highly unlikely to be generated in a broad range of ill-defined abnormal environments. The derivations in Chapter II hinge on a representation in which UQS events must be generated in abnormal environments one-at-a-time in sequence, and on the order in which those events would have to be inadvertently generated. Any forms of inadvertent

[17] Thus, "the unique signal" per se is not communicated as an entity. Rather, only one "UQS event" exists at a time from the standpoint of the UQS communication channel.

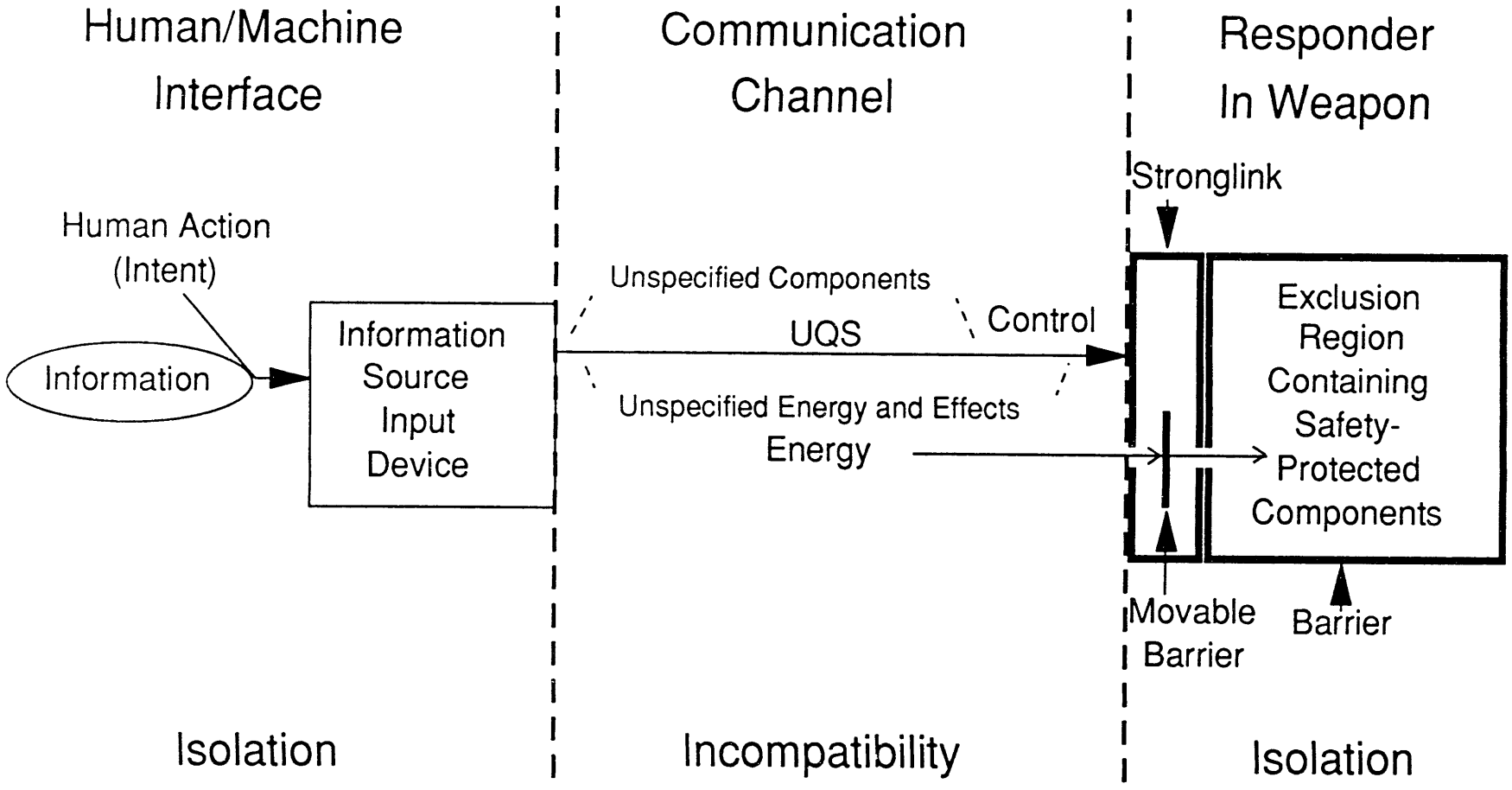


Figure III-1

A Safety Subsystem

generation that created more than one UQS event by a single, common action would invalidate the concept, and could degrade safety.

Therefore, it is important that the UQS communication channel be a true "passthrough" communication channel, i.e., utilized in such a manner that any UQS events that may be generated inadvertently in abnormal environments are forced to occur in one-at-a-time sequence. Furthermore, it is also important that the UQS communication channel not permit the order of UQS events to be altered anywhere between the point at which they were generated and the stronglink's UQS discriminator, which is the only place in the entire safety subsystem where "decisions" are made. Note that buffering and re-ordering can be inherent in any communication system, especially in an abnormal environment, if the mode of information input is not carefully controlled.

Rather than carefully designing, analyzing, testing, and controlling the UQS communication channel to be predictable in a broad range of ill-defined abnormal environments, the normal-environment channel is utilized as a "no knowledge" channel, i.e., in such a way that no more than one UQS event is ever present at one time in the channel. By this means, inadvertent generation is inherently limited to one event at a time. Also, if only one UQS event is present at a time, it is impossible for the order of the events to be altered, even though the UQS communication channel may be operating unpredictably as a result of abnormal environments.

A useful analogy is a telephone system, which has the capability of either processing complete messages in a single call, or simple message constituents in separate calls. If the system is entrusted with an entire message, there can be no assurance that a similar or identical message does not exist that could be catastrophically mis-routed in an abnormal environment, or that parts of the message will not be re-ordered (e.g., through packet transmission), unless the details of the communication channel are known in normal environments and assured in abnormal environments. However, if the system is given information one simple entity for passthrough at a time in separate calls, only the uncertainty of the pattern sequence matters, and nothing else need be known about the communication system, which simplifies assessment and makes safety assurance possible. (Further elaboration is given in Ref. 1.)

In addition to communicating each UQS event individually, the UQS communication channel should not contain any form of pre-stored knowledge of the correct pattern of the UQS.[18] In abnormal environments, such pre-stored knowledge could have the potential to act as a source of the correct pattern, or to act as a filter preventing inadvertently generated incorrect patterns from being communicated and thus preventing the stronglink from locking up in a safe condition in an accident. Communication of each UQS event in turn must go on without regard to what events may or may not have

[18]The term "knowledge of the correct pattern" is not restricted to a copy of the complete pattern. Any information that would allow parts of the correct pattern or identification of incorrect patterns should be precluded.

been communicated previously. Therefore, the second nuclear safety consideration for utilizing the UQS communication channel is:

*** **There should not be any form of pre-stored knowledge of the correct pattern of the UQS in the UQS communication channel.**

The UQS information source input device has knowledge of the UQS pattern; the communication channel should not. Attempts to merge the two functions lead to prestorage. One of the tests for detecting pre-storage in a UQS communication channel is to ask the question: "What changes would be needed to accommodate a UQS with a different pattern?" Any point in the channel that would require a change is a point with pre-stored knowledge pertaining to the correct pattern of the UQS.

The third nuclear detonation safety consideration for utilizing the UQS communication channel relates to the first two considerations, as well as to the fundamental UQS principles. The safety designed into the UQS would be jeopardized if the UQS communication channel were to do anything differently based on knowledge of the position of a UQS event in the sequence. Treating a subsequent UQS event in any way different than a prior one would be a form of pre-storage of pattern information, as well as not complying with the safety principle that each UQS event be an independent member of a sequence. Thus, the third nuclear safety consideration for utilizing the UQS communication channel is:

*** **Each UQS event must be processed the same as all other UQS events.**

This safety consideration has two obvious implications. First, no component of the UQS communication channel should count the UQS events or any portion of the events as they are transmitted through. Second, the formats of the UQS events themselves should not contain any indication related to the position of any event in the sequence.

Restriction from counting the UQS events as they are processed should not burden any component in the UQS communication channel. The channel's task is simply to transmit a UQS event from the operator's UQS information source input device to the stronglink, then to wait for the next event and repeat the process. The information source input device and the UQS discriminator at the two ends of the UQS communication channel need to be able to tell when all UQS events have been processed. The channel between the source and discriminator does not.

Restriction from position indication in UQS event formats eliminates the possibility that a buffering device[19] might (possibly inadvertently) store or retrieve UQS events in the order determined by the counters, rather than in a first in, first out order. If employed, such changing of the order of the UQS would undermine the engineering of the pattern of the UQS described in Chapter II.

Digital UQS communication channels frequently have the capability of transmitting a message (a single UQS event) more than one time for

[19]Storage (buffering) of the UQS pattern is discussed in Appendix AII.

reliability. In these cases, some method is required to distinguish a repeated UQS event from the next event in the sequence. It is not necessary to use a position counter in each UQS event's format to make this distinction. Rather, a one-bit flag can be complemented each time a new event is transmitted. The receiver then compares the one-bit flag of a newly received UQS event with that of the previously received event and, if they are the same, treats the newly received event as a repeat; or if they are different, steps irreversibly to the next event. Thus, a receiver can have the capability necessary to correct process-repeated UQS events without also having an undesirable ability to alter the sequence of incoming events.

Summary of Nuclear Safety Considerations for Utilizing the UQS Communication Channel

The three nuclear detonation safety considerations for utilizing the UQS communication channel to transmit a UQS are:

1. **Each UQS event must be communicated individually.**
2. **There should not be any form of pre-stored knowledge of the correct pattern of the UQS in the UQS communication channel.**
3. **Each UQS event must be processed the same as all other UQS events.**

No Constraint on Formats of UQS Events

The UQS event format is not safety-critical because it communicates only one UQS event. Within the UQS communication channel, it can be represented in any applicable manner (e.g., 28v DC pulses, digital messages, optical signals, etc.). This gives UQS communication channel designers a free hand in choosing how they wish to transmit each UQS event. A given type of UQS event may be represented by one format at one point in the channel, and a different format at another point. The act of changing the format of a UQS event is called "translation". Formats may be translated from point to point along the channel so long as the first nuclear detonation safety consideration for utilizing the UQS communication channel is complied with, that is, a format translator may operate on only one UQS event at a time. The translated format of one UQS event must be transmitted down the channel before another event may be accepted by the format translator.

Implementing Nuclear Safety Considerations for Utilizing the UQS Communication Channel

UQS communication of events as separately generated analog signals (e.g., 28v DC pulses, either short duration or long duration for the two different UQS event types) is straightforward. Such signals are ordinarily transmitted via a single hard wire (plus return). In these analog UQS communication channels, basic physics assures that each UQS event (voltage pulse) must be communicated individually so that a single, common action can inadvertently generate only one UQS event, and any sequence of pulses that might be received by the stronglink's UQS discriminator must have been generated in the order received. A wire intrinsically does not allow simultaneous multiple signals, nor does it allow the order of pulses to change.

However, digital processing in UQS communication channels[20] introduces potential for not complying with the safety principle that each UQS event must be communicated individually. If this potential were realized, more than one UQS event could be inadvertently generated as the result of a single, common action, and the order of UQS events could be inadvertently changed as they pass along the UQS communication channel. There is a human inclination, driven by desire for efficiency, to consider compressing more than a single UQS event into one digital word or message. Such compression does not comply with the first safety consideration for utilizing the UQS communication channel. Compression of multiple UQS events into one computer word adds a susceptibility to premature UQS generation by opening the opportunity for an inadvertent fetch of a portion or all of the UQS from a single storage location where it may have been stored for some unrelated function. Compression of multiple UQS events into a single digital message adds the possibility of a single action causing inadvertent generation of the correct pattern of the UQS (or a portion thereof) by erroneously accepting a message on the digital "party line" bus which was sent by some unknown and unknowable transmitter intended for some unknown and unknowable receiver.

In contrast to analog channels, digital communication channels do not intrinsically comply with the nuclear safety considerations for utilizing the UQS communication channel.[21] Digital implementations make it even more important to assure the use of sound principles. If only one UQS event is communicated at a time over a digital communication channel (it is constrained to a "no-knowledge" channel), the safety considerations are complied with and the safety designed into the UQS is preserved, while at the same time the impractical task of analyzing the UQS communication channel's response to abnormal environments is avoided (analogous to an analog channel). Thus, computer processors in the channel are restricted to acting as no more than UQS event format translators. The complex processing a computer would otherwise be capable of is precluded because only information relating to a single UQS event is available at any one time.

It is fundamental to this approach that the highest level at which information is processed should represent no more than one single UQS event. For typical digital UQS message-oriented communication channels, this means that the 24 UQS events for each UQS are intended to be sent with one event per message. Moreover, UQS principles no longer apply and cannot be invoked to assure safety in abnormal environments if two or more UQS events are processed at the same time at any point in a digital UQS communication channel.

---

[20]The UQS communication channel includes everything between the operator's information source input device and the stronglink in the weapon, including computer processors.

[21]Several examples of failure to comply with nuclear safety considerations in UQS communication channels are discussed in Appendix A-II.

Examples of Digital Representations of UQS Events

The size of the digital "package" that represents a UQS event is dependent on the particular digital component involved. Three examples follow:

Example One: A computer's internal buses typically can process only one digital word at a time. Likewise, a computer's working registers are limited to one word at a time. The word length is a function of the processor and can be as short as four bits or as long as sixty bits or more. But, no matter how long or short it may be, a digital word is the highest level at which information is processed, and therefore, should represent no more than one single UQS event.

Computers have the added capability to process less than a full word as a unit. For example, the terms "bit," "byte," or "short word" may be used to designate these fragments. Inasmuch as the capability still exists to process a full word at one time, the full word must be restricted to representing one UQS event because a single operation at the word level processes multiple bits, bytes, or short words.

Example Two: Digital communication buses connecting several components, each with its own processor, are usually organized to carry one digital message at a time. Each message includes a header containing the address of the intended recipient and other overhead information. Several (oftentimes, many) digital words are available for data. Although just one such digital message obviously has the capacity to carry much, if not all, of the data needed to re-generate the UQS sequence of events, nuclear safety considerations for utilizing the UQS communication channel restrict the message to no more than one single UQS event. Communication efficiency must not invalidate the nuclear detonation safety concept.[22]

Example Three: Although encryption does not enhance abnormal-environment nuclear detonation safety, it is sometimes necessary to transmit a UQS across an encrypted communication channel for security reasons. This is possible where encryption of data is done independently on a group of data words called a block. Each block is encrypted together, but separate from and independent of adjacent blocks. Thus, an encryption block is the highest level at which information is processed and should represent no more than one single UQS event. Again, efficiency must not invalidate the nuclear safety concept.

An Application of Unrestricted UQS Event Formats: Digital Error Detection and Correction

As discussed previously in this chapter, the formats by which UQS events are distinguished are not safety-critical. UQS event formats may be represented in any applicable manner and may be changed (translated) from point to point along a UQS communication channel. An important benefit of this freedom becomes available in UQS communication channels employing digital processing.

[22] In reality, the small number of messages (24) and the minimal number of times a UQS would be sent have little impact on a modern, high-speed digital communication bus.

Most digital communication channels incorporate some form of error detection, the simplest and most common example being parity checking. More involved algorithms, such as cyclic redundancy checks (CRC) and error-detection codes are sometimes used to detect errors and, in some cases, are extended to provide a level of error correction as well. These reliability techniques may be fully used when communicating UQSs, so long as each UQS event is processed alone.

The effect of digital error detection and correction on the communication of a single UQS event is to broaden the tolerance band on the definition of the type of the event. In other words, several different digital words would all represent an 'A' type UQS event. This is fundamentally no different than the analog situation where a range of pulse amplitudes/widths all are discriminated as the same UQS event type. In the analog case, the tolerance range is typically quite broad, and furthermore, is not assured to remain the same in abnormal environments.

Inasmuch as the UQS subsystem safety is controlled by the safety provided by the stronglink,[23] the same wide tolerances on UQS event types that are applied at the stronglink may also be applied in the UQS communication channel. Permitting many different digital words to consistently represent the same UQS event type would be of concern only if a particular word were not always interpreted as the same event type because only the pattern of the UQS is engineered to be highly unlikely to be generated in abnormal environments. Individual UQS events are easily generated in some portions of a UQS communication channel, among which are the analog wires leading to the stronglink.[24] Therefore, there is no advantage in attempting to preclude the generation of individual UQS events elsewhere in a UQS communication channel.

In both the digital and the analog cases, the UQS events use only one of many "dimensions". It is obvious that a digital word can contain more information content than is needed to distinguish an 'A' type UQS event from a 'B' type. In a sense then, one dimension is allocated to the definition of the UQS event type, while other dimensions are available for further information content. While perhaps not as obvious in the analog case, more dimensions are available for information content than the one needed to distinguish UQS event types. An example will help make the point. Consider a voice circuit with a microphone keyed by an operator. In an accident, this circuit could become connected to the wires leading to the stronglink's UQS input. Thus, the voice circuit would become an inadvertent generator. Only the length of time the carrier is keyed on would be discriminated by the stronglink's UQS discriminator. The modulation from the microphone would be ignored, although it would contain far more information content that the one, keying-time dimension allocated to the UQS. Both "Yes!" and "No!" could be discriminated as short pulses.

---

[23]However, the UQS communication channel can make the safety subsystem less safe if it undermines the UQS. This degradation can be especially severe if all events are not individually communicated.

[24]Stronglink UQS discriminators are analog.

In both the digital and analog cases, an accident would have to generate a sequence of events matching the pattern of the UQS in the one dimension allocated to the type of each event, regardless of the information content of the other dimensions.

One concern is that it is possible for a digital error detection algorithm to be specifically designed to process UQS events and that it might inadvertently incorporate some form of pre-stored knowledge of the correct pattern of the UQS. This would not comply with the second safety consideration discussed earlier in this chapter. Such pre-storage could happen in at least two different ways.

One possibility for not complying with the prohibition against pre-storage of the pattern of the UQS is the use of a "lookup table".[25] A lookup table contains an entry for each possible incoming UQS non-event format that "corrects" that incoming format to either an 'A' UQS event type or a 'B'UQS event type, without regard to any generally applied UQS principles. Such a lookup table could "correct" the first received format (if it were a non event) into the correct first UQS event, the second received format (if it were a non event) into the correct second, etc., which would open a susceptibility to simple inadvertent generation of the correct pattern of UQS events.

A second possibility for not complying with the prohibition against pre-storage of the pattern of the UQS is that an error detection algorithm specifically designed to process UQS events could be designed to count events and use different "rules" depending on the position of the current event in the sequence of UQS events. This would not comply with this chapter's third nuclear safety consideration for utilizing the UQS communication channel.

There are at least two possible approaches to avoiding the concern that a digital error detection algorithm that is specifically designed just to process UQS events might incorporate some form of pre-stored knowledge of the correct pattern of the UQS. One approach is to use only a single designated bit to determine the type of UQS event and ignore the remaining bits. Another approach is to correct each incoming UQS event to whichever type is "closest", i.e., has the fewer mismatched bits. The latter approach is less attractive where the "distance" (number of differing bits) between the two event types is even (meaning that an error(s) could make the number of bits to be corrected the same for either event type). In this case, an additional algorithm would be necessary for handling these received entities. This algorithm would then be subject to the problems mentioned above.

In summary, digital error detection and correction applied in the same way to each single UQS event in sequence amounts to no more than a sorting process on each UQS event. That is, each incoming UQS event is sorted into either the 'A' group or the 'B' group based on some established characteristic (dimension) of the incoming event. There is no conflict with fundamental nuclear detonation safety principles inasmuch as the width of the tolerance band on UQS event formats is not safety-critical.

---

[25] Or, a complex algorithm duplicating the function of a lookup table.

Chapter Summary

The major payoff of the UQS approach to nuclear detonation safety in abnormal environments benefits the UQS communication channel, allowing nuclear safety in abnormal environments to be achieved at the level of the weapon system without requiring that the UQS communication channel be predictable in abnormal environments. To obtain this payoff, three nuclear detonation safety considerations for utilizing the UQS communication channel to transmit a UQS should be complied with.

1. **Each UQS event must be communicated individually.**
2. **There should not be any form of pre-stored knowledge of the correct pattern of the UQS in the UQS communication channel.**
3. **Each UQS event must be processed the same as all other events.**

It is fundamental to this approach that the highest level at which information is typically processed should represent no more than one single UQS event (Ref. 1). Digital communication channels -- in contrast to analog channels -- do not intrinsically comply with the nuclear safety considerations for utilizing the UQS communication channel. It is necessary to restrict the usage of digital UQS communication channels such that the highest level at which information is processed -- be it a digital word, or a digital message, or an independent encryption block -- represents only one UQS event.

However, the format that defines a UQS event type, i.e., 'A' or 'B', is not safety-critical and can be represented in any applicable manner. UQS event formats may be translated from point to point along the UQS communication channel so long as the first and third safety considerations for utilizing the channel are complied with; a format translator may operate on only one UQS event at a time and must operate uniformly on all events in the sequence. A resulting observation is that digital error detection and correction does not conflict with any of the four nuclear safety considerations so long as each UQS event is processed alone and consistently.

Ref 1. "Separate-Event Unique Signal Transmission," J. A. Cooper, SAND90-0315, December, 1991.

Appendix I

THE UQS SOURCE

Introduction

The fundamental nuclear detonation safety goal in the design of modern weapon systems is to assure, at a high level of confidence, that the nuclear weapon will not produce a premature nuclear detonation when the weapon system is subjected to normal environments and to a broad range of ill-defined abnormal (accident) environments such as fire, crush, and electrical power. This safety goal can be divided into two basic objectives:

> In the absence of specific enabling inputs (the pattern of the UQS), the nuclear weapon must preclude, at a high level of assurance, a premature nuclear detonation in both normal and abnormal environments.
>
> In the absence of deliberate, precise human actions at the human/machine interface, the rest of the weapon system (e.g., aircraft, missile, ground control equipment) must communicate events separately (without buffering or non-uniform processing) in order to preclude, at a high level of assurance, premature application of the specific enabling inputs (the pattern of the UQS) to the weapon.

A weapon system can be no safer than its least safe element. The UQS source, if not carefully implemented, has the potential to undermine all the nuclear detonation safety efforts described in the other parts of this report.

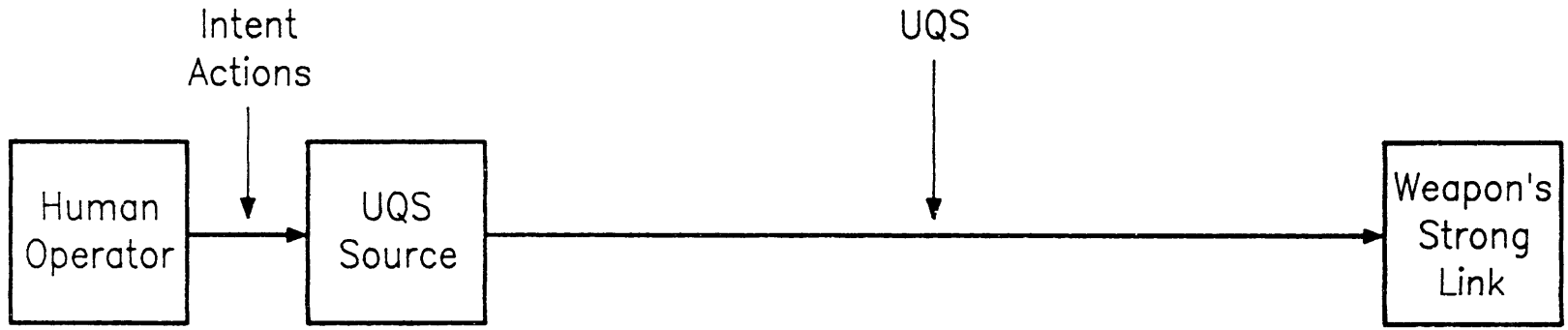
"Intent" and "Trajectory" Safety Subsystems

From the UQS viewpoint, safety subsystems that have been designed fall into three classes: those that employ UQS safety principles throughout, those that do not, and those that combine the above two classes. Figure AI-1 illustrates the distinction between the first two classes.

In the first class of safety subsystem, the human operator's human/machine interface is the UQS source. Abnormal-environment nuclear detonation safety for the entire communication channel from the human operator to the weapon's safety device is based on the UQS principles presented in this report. In the second class of safety subsystem, a remote UQS source is located "downstream" from the human operator's human/machine interface. Sensed environments from a weapon's trajectory cause generation or release of the UQS.

It has become customary to refer to the first class of safety subsystem as "intent" subsystems, and the second class as "trajectory" or "environment" subsystems. All safety subsystems must be traceable back to a human operator's action. Thus, all subsystems must have "intent." The real difference is that in those subsystems labeled "intent," the UQS is directly input by human intent actions; while in those labeled "trajectory"

"Intent" Safety Subsystem



"Trajectory" Safety Subsystem

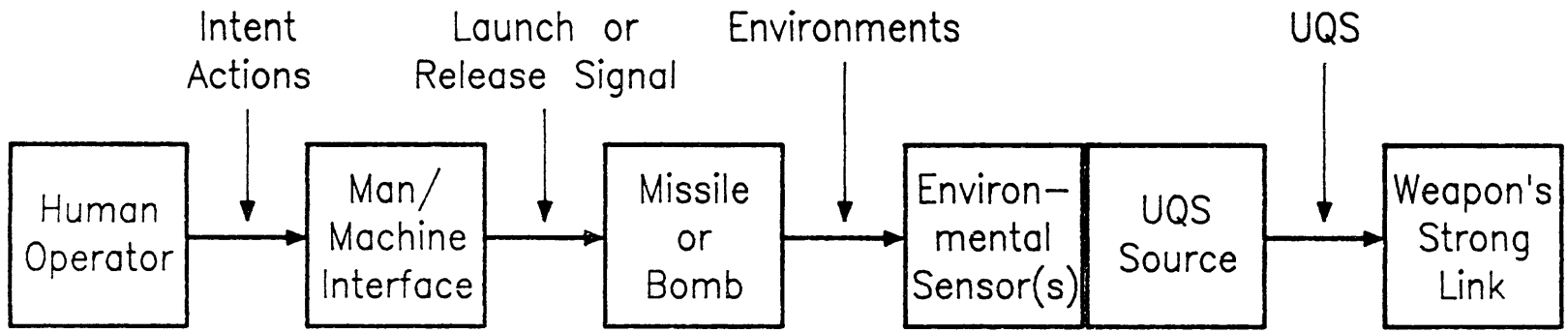


Figure AI-1
Comparison of "Intent" and "Trajectory" Safety Subsystems

or "environment", a human operator's intent action or actions start a trajectory, which creates environments, which in turn generate or release a UQS. There are potential pitfalls in this latter path (discussed subsequently).

In trajectory safety subsystems, both the environments (which generate or release the UQS) and the weapon launch or release signal (which initiates the environments) are safety-critical and therefore must meet stringent requirements for safety. Note that the advantage of intent safety subsystems is that they eliminate the dependence on the environment.

Nuclear safety considerations for UQS input at the human/machine interface and their implementation will be discussed in this appendix.

UQS Safety Considerations at the Human/Machine Interface

Nuclear detonation safety hinges on the assurance that the UQS will not be delivered accidentally or inadvertently to the weapon. Therefore, the major nuclear safety goal for the human/machine interface is to provide a high level of assurance that the UQS cannot be entered or generated by a broad range of ill-defined abnormal environments, nor inadvertently by an operator. Of course, when desired, the operator must be able to enter the UQS easily and reliably.

Thus, accidental or inadvertent entry of the UQS at the human/machine interface must be precluded. The method of entering the UQS at the operator's human/machine interface must be carefully engineered to attain a high degree of assurance that the safety characteristics are achieved. Safety concepts based on fundamental, straightforward principles should be used to simplify the design, analysis, test, and control efforts needed to obtain that high degree of assurance.

It must be recognized that hardware in the console at the human/machine interface, in the electronics behind the console, and in the rest of the UQS communication channel may be normal-environment equipment, uncertified and unpredictable in a broad range of ill-defined abnormal environments. Thus, there can be no design features to prevent transmission of the UQS in abnormal environments, after it is entered into the safety subsystem. Therefore, a basic safety premise is the following:

> Insertion of the UQS into the safety subsystem at the human/machine interface results in immediate loss of the abnormal-environment safety function provided by that subsystem.

Throughout the safety subsystem in the "safe" state, vital information[26] separation is a cardinal safety principle. The pattern of the UQS should not reside in the system, but should require deliberate, accident-resistant, human actions to insert it. To implement a vital information separation safety concept at the human/machine interface, several safety-related design considerations are important:

---

[26]In UQS discussions, the word "information" is used in a dictionary sense that is broader than the narrow sense used in communication theory.

Vital Information Separation: All of the information needed to generate the UQS pattern should be isolated from the weapon system until enabling of the weapon's stronglink is desired. Physical separation of the information from the human/machine interface should be significant and obvious. "Vital" means that the separated information should contain all the information contained in the pattern of the UQS itself, such that an event-by-event equivalency is achieved. Note that the fundamental safety principle of isolation employed at the human/machine interface is the same safety principle exemplified by the weapon's stronglink and barrier. Safety-critical information is isolated at the human/machine interface, while safety-critical energy is isolated at the weapon's exclusion region that protects components critical to producing a nuclear detonation. This is in contrast to the UQS communication channel discussed in the previous chapter, which utilizes the fundamental safety principle of incompatibility implemented by means of the pattern of the UQS and its communication technique.

No Pre-Storage: As in the UQS communication channel, there should be no form of pre-stored knowledge of the correct pattern of the UQS within the human/machine interface.

No Fail-Arm Concepts: The design of the human/machine interface should not depend on electronic circuits and computer algorithms that attempt to detect inadvertent insertion of the UQS and then inhibit its transmission for abnormal-environment safety. Such circuitry may malfunction and fail to detect or inhibit transmission in abnormal environments.

Positive Assurance Features: The human/machine interface should provide positive normal-environment design features to prevent inadvertent human action that results in insertion of the UQS. These features should include: 1) highly visible, obvious, continuous, and tamper-detection (e.g., seal wire) features to clearly identify the safety-critical function and to provide a clear indication that the UQS has not (or has) been inserted,[27] and 2) mechanical features to assure that casual, inattentive bumping or pressing by the operator will not cause UQS insertion. More important, there must be abnormal-environment-resistant design features (e.g., isolation of a UQS ROM key from the ROM-key reader).

Good Human Factors: When desired, the operator should be able to insert the UQS rapidly and accurately under normal environment conditions.

High Reliability: Once the UQS is inserted, the operator should have high confidence that it is correct, without the use of techniques that could undermine nuclear detonation safety.

UQS Implementation at the Human/Machine Interface

First-principle safety concepts must be clearly identified at the human/machine interface where the UQS is manually inserted into the weapon system. The major nuclear detonation safety goal is to assure that the UQS

[27]This is a safety, not security, function. The target is only the "friendly fiddler" not a determined adversary.

cannot be entered or generated at the human/machine interface by a broad range of ill-defined abnormal environments, nor inadvertently by an operator. Of course, when desired, the operator must be able to enter the UQS easily and reliably. Keyboard entry does not meet the aforementioned requirements. The disadvantages of keyboard entry are discussed in Appendix II.

The fundamental safety principle of isolation can be implemented by use of a separated component that has to be physically inserted into the safety subsystem in order to generate the pattern of the UQS. Figure AI-2 illustrates how the pattern of the UQS can be contained in a separated component, isolated from the safety subsystem. Some examples of such a separated component are a ROM plug or key, a tape cassette, a "smart" card, and a bar code which can be read optically.

For these examples, only when the nuclear weapon is to be employed would an operator insert the separated component into the UQS reader, which is the input to the UQS communication channel and thus, the safety subsystem. A simple, non-safety-critical "Enter" action -- or perhaps the act of insertion itself -- would initiate the UQS reader to read out each UQS event one-at-a-time and input it in turn into the UQS communication channel for transmission to the weapon.

The UQS reader by itself -- that is, without the safety-critical information contained in the separated component and without buffering[28] -- is incapable of generating the correct pattern of the UQS. Therefore, the UQS reader could be made not safety-critical. Rather, it could be the beginning of the UQS communication channel. As such, its hardware design would need only consider normal-environment predictability. However, as part of the UQS communication channel, the UQS reader must comply with the nuclear detonation safety considerations for utilizing the UQS communication channel developed in the previous chapter.[29] Note also that no form of pre-stored knowledge of the correct pattern of the UQS should be in the UQS communication channel.

The pattern of a UQS is safety-critical, while the individual UQS events and their formats are not safety-critical. Inasmuch as the separated component must contain all safety-critical information, it follows that it must contain the complete pattern of the UQS. That is, the separated component contains all of the events in the UQS in their correct sequence. Because the formats identifying each UQS event in the separated component are not safety-critical, they may be freely selected to be compatible with the specific technology employed. The UQS reader, then, is really nothing more than a UQS event format translator[30] , translating each UQS event in turn from the format employed in the separated component into the format needed by the outgoing UQS communication channel.

---

[28]Discussed in the section of Appendix AII, titled "Beyond the UQS Communication Channel: Storage (Buffering) of the Pattern of a UQS".

[29]One example is a bar-code reader, where bars are read one-at-a-time and transmitted separately without buffering.

[30]Format translators are discussed in the section titled "No Constraints on Formats of UQS Events" in Chapter III.

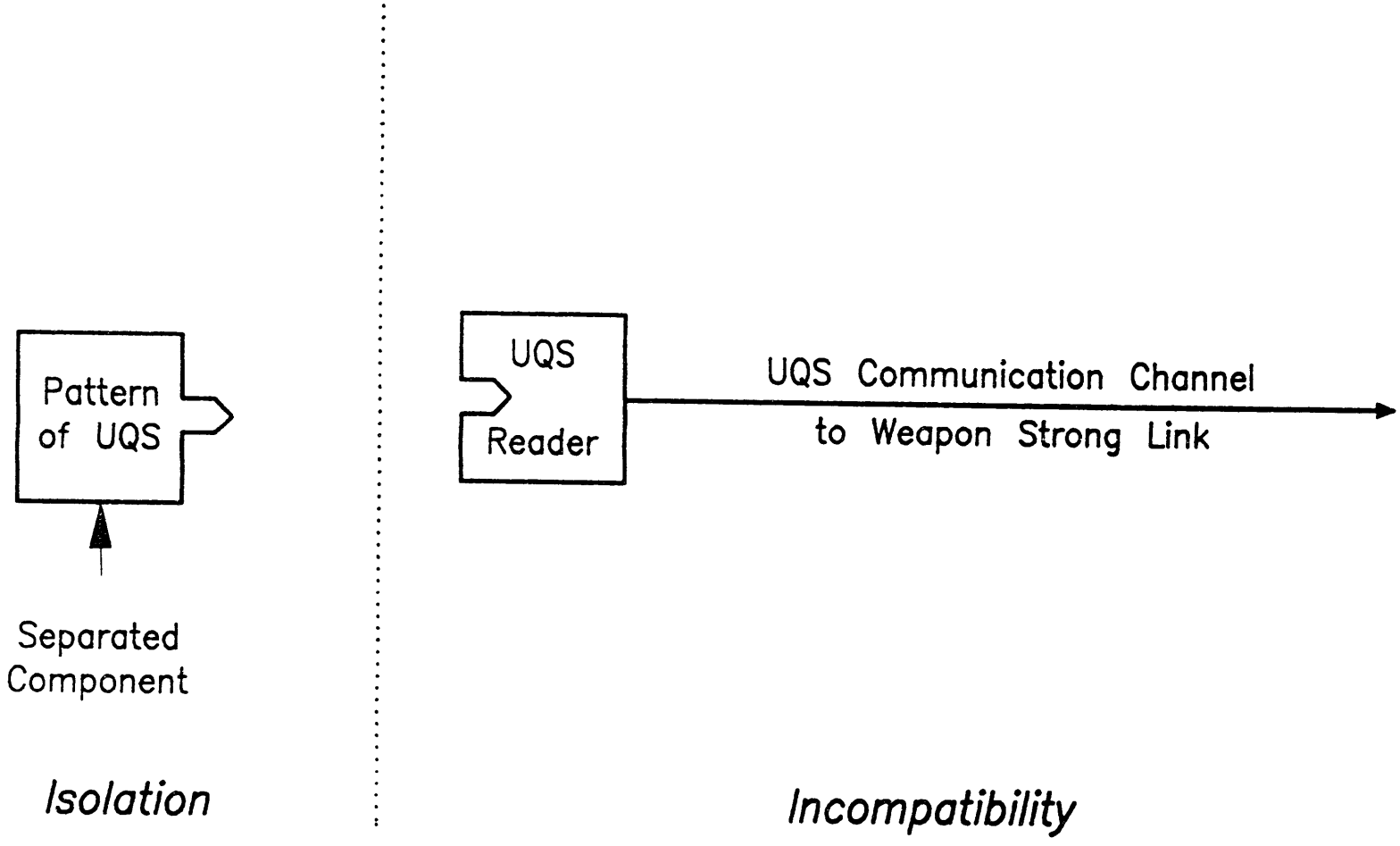


Figure AI-2
Separated Component at Human/Machine Interface

Thus, the separated component approach can provide assured isolation of the pattern of the UQS in normal and abnormal environments and allows a practical, reliable, and easy method for an operator to enter the UQS when that is desired.

Appendix AII

POSTSCRIPT ON PITFALLS

Introduction/Warning

The material presented in this appendix has been deliberately segregated from the main body of the report because it collects pitfalls which must be avoided. The main body of this report is intended to be a guide to sound implementation of the UQS concept. This appendix takes the opposite approach by presenting examples of unsound implementations. The intent is that known pitfalls not be repeated in future implementations of the UQS concept. UQS principles presented in the main body of this report are invoked throughout this appendix without elaboration.

The "Forbidden Format" Concept

One early 1970s idea for a design approach for a unique signal (UQS) was the "forbidden format" (or simply recognition of a "unique" pattern). The thought was that, if an electrical waveform or digital representation could have been found which had never been used (and would never be used) in any device associated with nuclear weapons, that pattern could have been used as a UQS. The intent was to publish the selected pattern with a warning that it was not permitted to be designed into any device of any kind, hence the name.

Two safety concerns became evident with this approach, and led toward development of the UQS concept described in this report. First, this approach would have required that the entire weapon system be treated as safety-critical in abnormal environments. Everything in the entire weapon system would have had to have been carefully designed, analyzed, tested, and controlled to assure that the forbidden pattern would not have been produced in a broad range of ill-defined abnormal environments.

Second, even in normal environments, it was found to be impossible to identify a pattern that no designer would ever want to use. This leaves the potential for a catastrophic vulnerability if it (one situation) occurred. Designers of devices that might become associated with nuclear weapons basically have the opportunity to do anything in their designs.

Abnormal-environment engineering analysis devoted to the forbidden format concept redirected the effort to develop a viable UQS concept, and led to the approach taken in Chapter I in which the formats of UQS events (each of which is single-situation catastrophically vulnerable) are not required to be safety-critical.

The Precision Timing Concept

Closely related to the "forbidden format" concept is the concept of precision timing. A safety device could have been designed to respond to a "start" pulse and a "stop" pulse with a very close tolerance on the time interval between the two pulses. Pulses with any different interval

between them would not have operated the safety device, and could have caused it to lock up.

In accidents, the intervals between pulses appearing at the safety device might have been "random" so that the chosen interval would have been unlikely to have been generated. However, time intervals between pulses existing in any given weapon system are not random, rather, they depend upon details of the designs of multitudinous components and subsystems. Furthermore, those components and subsystems are expected to change from time to time as modifications and additions are made to the weapon system. The time intervals between pulses in any weapon system are truly unknown and unknowable. As pointed out in Chapter I, this does not mean that they are in any sense random. This leaves the potential for a single-situation catastrophic vulnerability.

The Parallel Inputs Concept

Another concept that could have been selected is parallel inputs. The concept is to process separate parallel inputs, with the correct order of appearance determining the unique pattern. Any other order would result in lockup.

Controlling the positions of the input terminals on the safety device to assure that they were not in the order required to operate the device would have been straightforward. However, such a device would have required cabling with parallel conductors. Controlling the cabling would not have been straightforward. The entire communication channel from the operator's human/machine interface to the safety device would have had to have been carefully designed, analyzed, tested, and controlled to assure that the order of the conductors was safe and would remain so in a broad range of ill-defined abnormal environments. Such a requirement would have defeated the objective of the UQS which is to remove the UQS communication channel from abnormal-environment safety concern.

The parallel inputs concept can be analyzed using the methodology developed in Chapter II. Assume ten pulses, which may be given any labels. For simplicity, consider ten ordered alphabetic letters. Thus, the pattern of the parallel inputs can be described as:

A B C D E F G H I J

Counting pairs of pulses following the procedure in Chapter II yields the following table:

		Following Pulse									
		A	B	C	D	E	F	G	H	I	J
	A	0	1	0	0	0	0	0	0	0	0
	B	0	0	1	0	0	0	0	0	0	0
	C	0	0	0	1	0	0	0	0	0	0
	D	0	0	0	0	1	0	0	0	0	0
Leading	E	0	0	0	0	0	1	0	0	0	0
Pulse	F	0	0	0	0	0	0	1	0	0	0
	G	0	0	0	0	0	0	0	1	0	0
	H	0	0	0	0	0	0	0	0	1	0
	I	0	0	0	0	0	0	0	0	0	1
	J	0	0	0	0	0	0	0	0	0	0

Note that each leading pulse has only one following pulse. All other entries are zero. This leaves the potential for a single-situation catastrophic vulnerability.

Applying the P_{calc} formula of Chapter II:

$$P_{calc} = \left(\tfrac{1}{1}\right)^1 \times \left(\tfrac{1}{1}\right)^1 \times \left(\tfrac{1}{1}\right)^1 \times \left(\tfrac{1}{1}\right)^1 \times \left(\tfrac{1}{1}\right)^1 \times \left(\tfrac{1}{1}\right)^1 \times \left(\tfrac{1}{1}\right)^1 \times \left(\tfrac{1}{1}\right)^1 \times \left(\tfrac{1}{1}\right)^1 = 1.0$$

A Stepper Motor As a UQS Discriminator

A straightforward concept is to base a discriminator on a commercially available stepper motor. A particular motor that could have been selected has four steps per revolution. A gear train is attached so that twelve revolutions of the stepper motor (48 steps) are required to enable the device.

A 4-step stepper motor may be in any of four positions, which we will call A, B, C, and D for convenience. There are four corresponding inputs to the motor. The four positions are arranged circularly as follows:

```
A -- B
|    |
D -- C
```

From any position, the motor can move to an adjacent position, either forward or backward, but cannot jump to the opposite position. The step the motor will take (if any) depends on its current position and which input line is pulsed, as shown in the following table:

		Input Line A	B	C	D
	A|	A	B	A	D
Current|	B|	A	B	C	B
Position|	C|	C	B	C	D
	D|	A	D	C	D

Thus, the sequence of 48 steps to enable the device is:

A B C D A B C D A B C D A B C D A B C D A B C D
A B C D A B C D A B C D A B C D A B C D A B C D

In this repetitive pattern, counting pairs of steps following the procedure in Chapter II yields the following table:

		Following Step A	B	C	D
	A|	0	12	0	0
Leading|	B|	0	0	12	0
Step|	C|	0	0	0	12
	D|	11	0	0	0

As was the case with the "parallel inputs" concept, discussed in the previous section, each leading step has only one following step, here repeated a dozen times. All other entries are zero. This leaves the potential for a single-situation catastrophic vulnerability.

Applying the P_{calc} formula of Chapter II:

$$P_{calc} = \left(\frac{12}{12}\right)^{12} \times \left(\frac{12}{12}\right)^{12} \times \left(\frac{12}{12}\right)^{12} \times \left(\frac{11}{11}\right)^{11} = 1.0$$

A Keyboard as a UQS Source

Computer-type keyboards are sometimes used for a UQS source at the human/machine interface to make use of existing hardware in aircraft and other control consoles. One examples of this practice is input for the 47-event pattern of the multiple-try MC2969's UQS. In this approach, advantage is taken of knowledge of the number of groups of UQS events in the pattern. Since there are eight groups of events in the pattern of the MC2969's UQS, eight keystrokes are employed to input the entire pattern. The algorithm used compresses each of the eight groups of UQS events into a single hexadecimal digit representing the count of the UQS events in the group. A function downstream of the human/machine interface re-expands the eight hexadecimal group counts into the true 47-event pattern of the UQS.

The pattern of the MC2969's UQS is listed in Table II-1 of Chapter II along with the patterns of the other UQSs currently in use. This 47-event pattern is repeated here along with the 8 hexadecimal digits into which it is compressed:

AAAAAAAAAAA BB AAAAAAAAAAAAA BBB AAAAA BB AAAAAAA BBBB

B2D35274

This use of a keyboard as a UQS source, with its drastic compression and re-expansion of the pattern of the UQS, raises several nuclear detonation safety concerns. A P_{calc} analysis following the methodology developed in Chapter II and employed in previous sections of this appendix will be presented first. Further nuclear safety concerns will then be discussed.

Counting pairs of keystrokes following the procedure in Chapter II yields the following table:

		Following Keystroke						
		2	3	4	5	7	B	D
	2	0	0	0	0	1	0	1
	3	0	0	0	1	0	0	0
Leading	4	0	0	0	0	0	0	0
Keystroke	5	1	0	0	0	0	0	0
	7	0	0	1	0	0	0	0
	B	1	0	0	0	0	0	0
	D	0	1	0	0	0	0	0

With one exception -- the "2" key -- each leading keystroke has only one following keystroke. All other entries are zero. This leaves the potential for a catastrophic vulnerability.

Applying the P_{calc} formula of Chapter II:

$$P_{calc} = \left(\frac{1}{2}\right)^1 \times \left(\frac{1}{2}\right)^1 \times \left(\frac{1}{1}\right)^1 \times \left(\frac{1}{1}\right)^1 \times \left(\frac{1}{1}\right)^1 \times \left(\frac{1}{1}\right)^1 \times \left(\frac{1}{1}\right)^1 = 0.25$$

The first two factors come from the "2" key, and reflect the two different alternatives following a "2".

It may be tempting to include the effect of the nine hexadecimal digits missing from the pattern B2D35274. However, there is no assurance that such non-events would be generated in an accident. Nine additional rows and columns could have been included in the table of pair counts above, but they would have been filled with nothing but zeros. Again, the P_{calc} computation would have been unchanged. Appending more keys to the keyboard doesn't help.

Another nuclear detonation safety concern is that the vast majority of 47-event patterns can't be represented by a pattern of 8 group counts. As just one example, the simple pattern, ABABAB..., has far too many groups of events to be represented by a scheme which allows for only eight groups. This alternating pattern might be very likely to be generated in some accident situations; and if it were to be generated and communicated to the stronglink, the stronglink is assured to lock up in a safe condition in

both normal and abnormal environments. Preventing the pattern from being generated in abnormal environments removes an opportunity for the stronglink to lock up.

Figure AII-1 graphically illustrates the loss of patterns caused by retreating from 47 events to 8 hexadecimal group counts. The area of the large circle represents the 2^{47} = 140,737,488,355,328 different patterns of 47 events, the minimum number of patterns required to assure abnormal-environment safety. The area of the tiny circle on the left edge of the large one represents -- to the same scale -- the 16^8 = 4,294,967,296 different patterns of 8 hexadecimal group counts, even under the assumption that all sixteen group-count hexadecimal digits are available even though only seven different keys are required. Of course, applying more-safety-conservative assumptions would make the circle even more minute. The area of the large circle not covered by the small one represents the lost patterns.

Re-expanding a pattern of 8 group counts into the 47-event pattern of the UQS using pre-stored knowledge of the correct arrangement of event groups in the pattern acts as a filter eliminating most of the population of incorrect (safe) patterns to which an accident might have access.

There is a further safety concern. Most of the little circle is outside the large one. Only about two percent of the patterns of 8 group counts generate sequences of exactly 47 events. Some of the other 98% would not cause the stronglink to lock up, but could leave it advanced part way toward its enabled condition.

Other implementations of keyboards as UQS sources use different schemes to compress and re-expand the operator's input. All are subject to similar safety concerns and do not assure safety as is expected of a true UQS.

Furthermore, it is not just the UQS source that is undermined when the pattern of the UQS is compressed to fit a keyboard at the operator's human/machine interface, and later re-expanded to the full sequence of individual events making up the UQS. In many cases, the function that re-expands the compressed operator input into the separate events of the UQS is located near the nuclear weapon. Therefore, the entire communication channel from the operator's human/machine interface to the re-expansion module near the weapon is subject to the nuclear safety concerns outlined in this section.

In order to apply the UQS principles presented in the body of this report to a keyboard UQS source, it would be necessary to have the operator make one keystroke to generate each UQS event. Just two keys would be used, one to generate an 'A' type UQS event, and one to generate a 'B'. Such an approach is obviously impractical from a human factors reliability viewpoint, and has never been considered as part of the UQS concept.

The **unavoidable conclusion is that keyboards can't simultaneously satisfy both nuclear detonation safety and human factors considerations.** The solution is to avoid keyboards altogether. The separated component

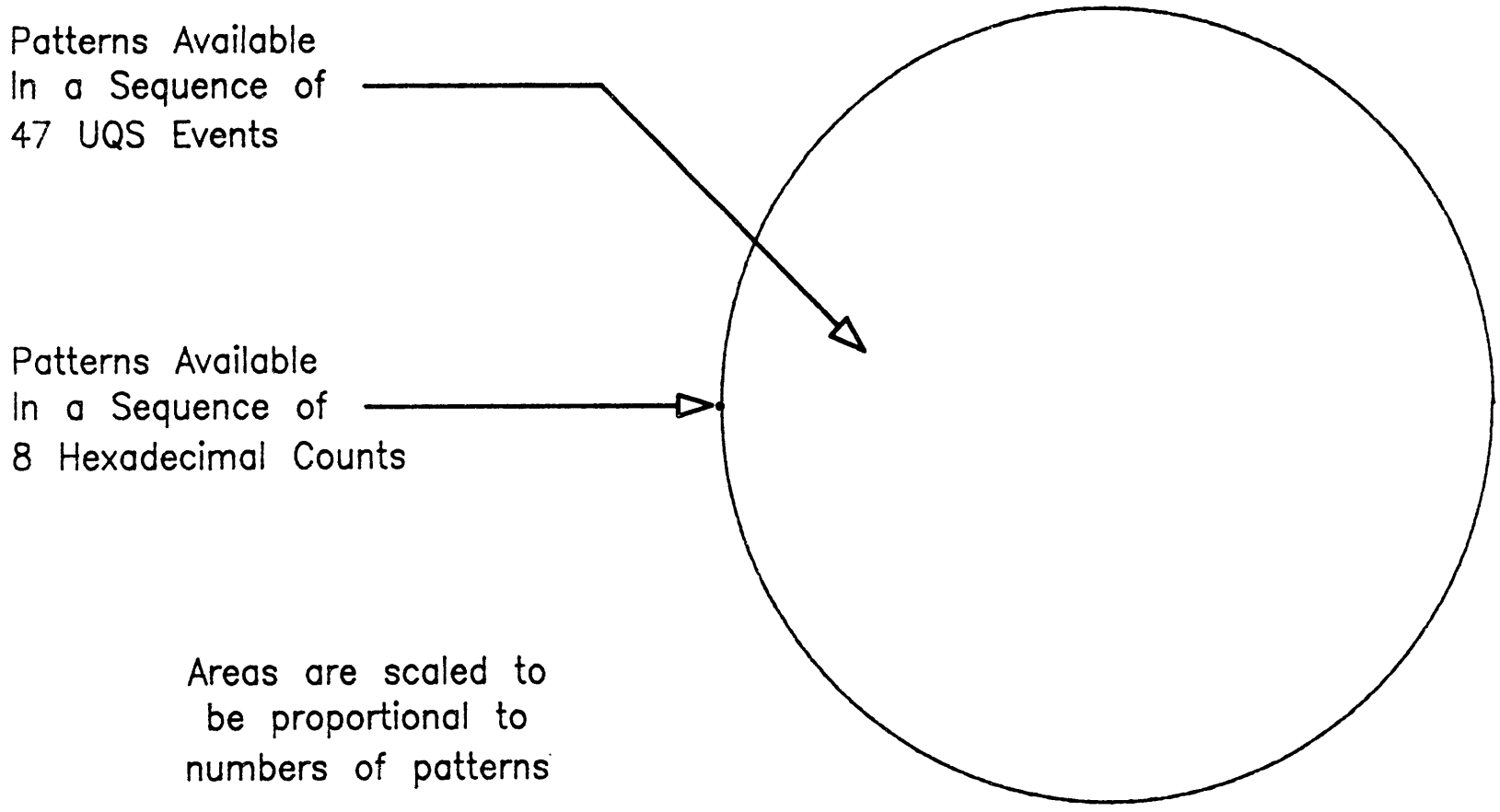


Figure AII-1
Loss of Patterns Caused by Retreating to 8 Hexadecimal Counts

approach, as described in Appendix AI, provides a means of satisfying all nuclear safety considerations, and at the same time avoiding human factors concerns.

Beyond the UQS Communication Channel: Monitoring the Safe/Enabled State of a Weapon UQS Buffer

Buffering has been cited as contrary to the UQS approach. However, one case in which the pattern of a UQS is buffered (albeit creating safety-critical attention) is that of a weapon with a single-try stronglink UQS discriminator preceded by a buffer for the pattern of the UQS. The purpose of the UQS buffer is to allow re-safing if the process leading to release of an aircraft-delivered weapon is aborted after the intent UQS(s) has been communicated from the operator in the aircraft. Designed weapon operation is such that incoming UQS events are buffered but not sent to the stronglink's UQS discriminator while the weapon is still on board the aircraft. Following release, UQS events are retrieved from the buffer and sent to the UQS discriminator to operate the stronglink from its initial, safe condition to its enabled condition.

To accommodate the possibility of an abort following UQS enablement -- with the aircraft returning to base with the weapon still on board -- provision is made for a "resafe" signal from the operator to the nuclear weapon. On receipt of this "resafe" signal, the contents of the weapon's UQS buffer are erased and replaced with the initial "safe" pattern.[31] It must be recognized that resafing is a normal-environment, reliability-mode operation.

Inasmuch as the operator in the aircraft has a capability to change the state of the weapon's UQS buffer from "safe" to "enabled" and back, it is reasonable to provide him with a means of monitoring the state of the buffer, both to provide him with human-factors feedback when he has initiated a change, and to allow him to check whether the buffer is in the state he desires at any time. A second reason for providing a capability to monitor the UQS buffer is its contribution to weapon system reliability; errors resulting from an unreliable UQS communication channel, or unreliable UQS input at the source input device can be detected and corrected by re-transmitting the UQS.

Logically, monitoring implies that somewhere in the weapon system there must be knowledge of what the UQS buffer contents should be for both the "safe" and the "enabled" states so that the actual buffer contents can be compared with the pre-stored versions. While pre-stored knowledge of the "safe" state poses no hazard to safety, pre-stored knowledge of the correct "enabled" state does. There are two nuclear detonation safety concerns.

First, pre-storage of the correct pattern of the UQS for monitoring purposes does not comply with the second nuclear safety consideration for utilization of the UQS communication channel discussed previously. In abnormal environments, such pre-stored knowledge could act as a source of the correct pattern and be released and transmitted to the stronglink's UQS

[31]Appropriate "safe" patterns are discussed in Chapter II.

discriminator.

Second, even if the pre-stored information does not directly drive the stronglink in an accident, it opens a potential for multiple tries.

In order to avoid both nuclear detonation safety concerns -- pattern source and multiple try -- a mechanism is needed which is assured not to make the pre-stored correct "enabled" version of the contents of the UQS buffer available to the safety subsystem in a broad range of ill-defined abnormal environments, but which will make it available when needed for monitoring the safe/enabled state of the buffer. The obvious method for safely accomplishing this[32] is to store the information needed to monitor the "enabled" state of the UQS buffer in the same location as the actual pattern of the UQS which is used to enable the weapon.

A method of monitoring the safe/enabled state of the UQS buffer that avoids nuclear safety concerns follows: First, on receipt of a "monitor" command, the weapon processor retrieves the contents of the UQS buffer and "echoes" it back through the UQS communication channel to the operator's information source input device interface. The design of the buffer is such that each UQS event must be retrieved separately.[33] However, the weapon processor may, if desired, compress the 24 retrieved UQS events into fewer than 24 digital words or messages (even into one) for echoing back to the source input device. Compression is permissible in this specific case because this is output from the buffer rather than input to it.

Second, the processor in the source input device compares the echoed UQS buffer contents with a pre-stored version of the "safe" echo. If they match, a "safe" indication is given to the operator and the monitoring process is complete. The correct version of the "safe" echo is always available in the processor at the source input device so that a "safe" state of the UQS buffer can be verified at any time. Specifically, the separated component containing the pattern of the UQS and the information needed to verify the "enabled" state need <u>not</u> be inserted into the source input device to accomplish monitoring of a "safe" weapon state.

Third, if the "safe" state is not matched and the separated component has not been inserted, an "unknown" or "not safe" indication is given to the operator and the monitoring process is complete. Note that this indication does not necessarily mean that the weapon is unsafe, only that it is not in the expected state.

---

[32]The use of a one-way transform as described in the next section may relieve the first (pattern source) concern but not the second (multiple try).

[33]Discussed in the previous section of this chapter.

Fourth,[34] if the "safe" state is not matched but the separated component has been inserted, the processor in the source input device compares the echoed UQS buffer contents with the version of the "enabled" echo from the separated component. If they match, an "enabled" indication is given to the operator and the monitoring process is complete. If neither the "safe" nor the "enabled" state is matched, an "unknown" or "not safe" indication is given to the operator and the monitoring process is complete.

Using a "One-Way" Transform to Monitor The Safe/Enabled State of a Weapon UQS Buffer

The previous sections describe buffering of the pattern of the UQS in a weapon and discusses nuclear detonation safety concerns associated with monitoring the safe/enabled state of the buffer. One commonly used, but non-ideal method is to pre-store in the weapon system information identifying the enabled state in what is known as a "one-way transform."

The procedure is for the warhead processor connected to the buffer to transform the contents of the buffer and transmit the results of that transformation operation back through the UQS communication channel. A comparison is made against a pre-stored copy of the transform of the correct enabled contents of the buffer. The intent is to avoid pre-storage of the correct pattern of the UQS at the location where the comparison is made.

The adjective "one-way" indicates that the transform is difficult, or preferably impossible, to invert. That is, it should not be feasible to derive the correct pattern of the UQS from the pre-stored transform. An obvious nuclear safety concern is verification that the specific transform employed is, indeed, one-way. It is not straightforward to assure that no subtle possibility exists that would allow the correct pattern to be derived from the pre-stored transform in some abnormal environment.

Another, less obvious, nuclear safety concern is the potential for multiple tries. Although incorporating a one-way transform might allow a designer to avoid pre-storing in the weapon system the correct pattern of the UQS that can enable the stronglink directly, it does not eliminate the safety concern for multiple tries.

The buffer (separated until intended use) monitoring method outlined in the previous section avoids nuclear safety concerns without requiring use of a one-way transform.

[34]This step contributes only to reliability, not safety, and may be omitted if the UQS communication channel and the UQS input at the source input device are adequately reliable.

Distribution:

20	O. E. Jones
25	R. N. Brodie
300	R. L. Schwoebel
303	J. L. Duncan
323	R. G. Easterling
323	K. V. Diegert
324	P. E. D'Antonio (7)
326	G. L. Lane
331	S. D. Spray (10)
331	J. A. Cooper (30)
332	G. A. Sanders (11)
333	R. E. Smith (10)
334	G. C. Novotny
335	J. M. Sjulin
336	E. M. Austin
361	R. F. Hahn
362	K. D. Flynn
363	J. N. Middleton
364	Oscar Hernandez
365	E. A. Disch
367	R. M. Oelsner
2000	H. W. Schmitt
2300	R. D. Andreas
2301	M. K. Parsons
2313	T. L. Evans
2314	M. J. Mundt
2337	W. D. Williams
2500	G. N. Beeler
2571	T. J. Williams
2600	J. H. Stichman
2615	J. M. Moore
2615	L. J. Dalton
2641	S. B. Martin
2643	R. S. Urenda (5)
2645	W. R. Leuenberger (5)
2665	D. H. Schroeder
4100	G. R. Otey
5000	R. L. Hagengruber
5003	J. F. Ney

5100 W. C. Nickell
5111 W. J. Patterson
5115 J. O. Harrison
5147 G. L. Maxam (5)
5161 J. A. Andersen
5161 K. Oishi
5165 J. M. Freedman
5166 R. C. Hartwig
5167 M. A. Rosenthal
5200 E. E. Ives
5202 D. J. Bohrer
5203 C. C. Burks
5205 T. S. Edrington
5209 E. T. Cull
5355 R. G. Miller
5361 M. H. Reynolds
5362 D. R. Henson
5375 C. T. Oien
5514 Al Hachigian
5700 M. J. Eaton
5702 W. R. Reynolds
5800 J. L. Wirth
5801 K. D. Nokes
5802 M. W. Callahan
5803 J. P. Abbin
7141 S. A. Landenberger (10)
7145 Document Processing (8) for DOE/OSTI
7151 G. C. Claycomb (3)
8000 J. C. Crawford
8100 M. E. John
8523 Central Technical Files
9332 A. B. Church
9511 S. K. Fletcher

Col. William H. Oakley, Director of Nuclear Surety
Det. 1, AFSA/SEN
Kirtland AFB NM 87117-5000

Col. Thomas G. Lauther
Det. 1, AFSA/SENS
Kirtland AFB NM 87117-5000

Col. Burl E. Hickman
Det. 1, AFSA/SENA
Kirtland AFB NM 87117-5000

Lt. Col. John Waskiewicz, AFISC/SNAA
Det. 1, AFSA/SENAA
Kirtland AFB NM 87117-5000

Capt. James Schoeneman
Det. 1, AFSA/SENA
Kirtland AFB NM 87117-5000

Keith Baird
Army AMCPM-NUC-AFO
Kirtland AFB NM 87117

Brigadier General
ASC/CV
Wright-Patterson AFB OH 45433-6503

Johnny Davis
ASC/EMSV
Wright-Patterson AFB OH 45433-6503

Capt. Marcel DeGraaf
ASC//VFAI
Wright-Patterson AFB OH 45433-6503

Major Walter Sorensen
ASC/VFAI
Wright-Patterson AFB OH 45433-6503

Jim Spieth
ASC/ENASD
Wright-Patterson AFB OH 45433-6503

Charles Stevens
ASC/YGES
Wright-Patterson AFB OH 45433-6503

Charles Sweet
ASC/ENASD
Wright-Patterson AFB OH 45433-6503

Glen Binns
DOE/AL NESD
Kirtland AFB NM 87185

Jerome H. Grayson, Director NESD
DOE/AL
Kirtland AFB NM 87185

A. A. Nichols
DOE/AL NESD
Kirtland AFB NM 87185

Bill Pecsok
DOE/AL NESD
Kirtland AFB NM 87185

Steve Guidice
DOE/AL NESD
Kirtland AFB NM 87185

Dave Finley
DOE/AL NESD
Kirtland AFB NM 87185

Ben Corley
DOE/AL NESD
Kirtland AFB NM 87185

Maximo Barela
DOE/AL NESD
Kirtland AFB NM 87185

CDR Tom Walker
Field Command, Defense Nuclear Agency
FCFA
Kirtland AFB NM 87115-5000

CDR Gene Haney
Field Command, Defense Nuclear Agency
FCFA
Kirtland AFB NM 87115-5000

Glenn Coleman, Commanding Officer
Naval Air Warfare Center, Aircraft Division
CODE 924
6000 E. 21st Street
Indianapolis, IN 46219

Roger Buettell
Naval Weapons Evaluation Facility
ATTN: A245
2050 2nd St. SE
Kirtland AFB NM 87117-5000

Michele Hedrick
Naval Weapons Evaluation Facility
ATTN: A245112
2050 2nd St. SE
Kirtland AFB NM 87117-5000

Commanding Officer
Naval Weapons Evaluation Facility
ATTN: A24
2050 2nd St. SE
Kirtland AFB NM 87117-5000

Jack Parker
Naval Weapons Evaluation Facility
ATTN: A 245217
2050 2nd St. SE
Kirtland AFB NM 87117-5000

John Lederer
OL-NS/EN
1651 First St. SE
Kirtland AFB NM 87117-5617

James Sweeney
OL-NS/ENN
1651 First St. SE
Kirtland AFB NM 87117-5617

Al Solomon
OL-NS/ENX1
1651 First St. SE
Kirtland AFB NM 87117-5617

Billy Stearnes
OL-NS/ENB
1651 First St. SE
Kirtland AFB NM 87117-5617

R. Dayhoff
OL-NS/ENBS
1651 First St. SE
Kirtland AFB NM 87117-5617

Kay Fick
OL-NS/ENN
1651 First St. SE
Kirtland AFB NM 87117-5617

Theresa Isaacson
OL-NS/ENBS
1651 First St. SE
Kirtland AFB NM 87117-5617

Mark LeDoux
OL-NS/ENN
1651 First St. SE
Kirtland AFB NM 87117-5617

Ron Lucero
OL-NS/ENX2
1651 First St. SE
Kirtland AFB NM 87117-5617

Al Matteucci
OL-NS/ENX1
1651 First St. SE
Kirtland AFB NM 87117-5617

Jerry Villane
OL-NS/ENBS
1651 First St. SE
Kirtland AFB NM 87117-5617

Stanford Gooch
STRATCOM/
Offutt AFB NE 68113-5001

Dr. James M. Turner, Assoc. Director for Weapons Safety
DOE DP-20.1
Germantown MD 20874

Vic Johnson
DOE DP-20.1
Germantown MD 20874

Joel Smith
DOE DP-20.1
Germantown MD 20874

Dave McVey
DOE NWC/WSC
Germantown MD 20874

Stanley Keel
Special Assistant for Nuclear Weapons Safety ATSD (AE)
The Pentagon, Room 3C124
Washington D.C. 20301-3050

☆ U.S. GOVERNMENT PRINTING OFFICE 1992—775-122/80170

END

DATE FILMED

9/30/93