Conf-9107215--1

WSRC-MS--91-275
DE92 009874

CRITICALITY SAFETY AND FACILITY DESIGN CONSIDERATIONS (U)

by

W. R. Waltz

Westinghouse Savannah River Co.
Savannah River Site
Aiken, South Carolina

A paper proposed for presentation at the
Nuclear Criticality Safety Short Course(Sponsored by Univ. of NM)
Albuquerque, New Mexico
July 10, 1991

This paper was prepared in connection with work done under Contract No. DE-AC09-89SR18035 with the U.S. Department of Energy. By acceptance of this paper, the publisher and/or recipient acknowledges the U.S. Government's right to retain a nonexclusive, royalty-free license in and to any copyright covering this paper, along with the right to reproduce and to authorize others to reproduce all or part of the copyrighted paper.

CRITICALITY SAFETY AND FACILITY DESIGN CONSIDERATIONS

W. R. WALTZ

June, 1991

For presentation at the Nuclear Criticality Safety
Short Course on July 8 – 12, 1991 in
Albuquerque, N.M.

CRITICALITY SAFETY AND FACILITY DESIGN CONSIDERATIONS

SLIDE 1 - INTRODUCTION

Operations with fissile material introduce the risk of a criticality accident that may be lethal to nearby personnel. In addition, concerns over criticality safety can result in substantial delays and shutdown of facility operations. For these reasons, it is clear that the prevention of a nuclear criticality accident should play a major role in the design of a nuclear facility.

In the brief time available, I have selected for discussion several topical areas, as shown in Slide 1. The emphasis will be placed on engineering design considerations in the prevention of criticality. The discussion will not include other important aspects, such as the physics of calculating limits nor critiality alarm systems.

SLIDE 2 - PROCESS PARAMETERS AND CONTROL METHODS

Nuclear criticality safety is achieved by controlling one or more parameters of the system within critical limits (ANSI/ANS-8.1). A "controlled parameter" is defined as one that is kept within specified limits (ANSI/ANS-8.1).

One of the major tasks in the design process is deciding which parameters will be controlled parameters. (In setting limits for the controlled parameters, the other parameters that influence criticality are assumed to reside at a worst case condition for criticality). In a large scale production facility, it is common that the particular parameters selected for control will change depending upon the point in the process.

Slide 2 lists eight common criticality "control methods," where the name attached to each identifies a controlled parameter. In design, the selection of which parameters to control will be influenced by several factors, including the facility throughput requirements. For example, it may be quite practical to use geometry control in a case where throughput requirements are small, while this method may not be practical at much higher throughputs levels.

In making selections it is important, however, to recognize that the various criticality control methods are not equally preferred from the standpoint of criticality safety. To explore this point, I will discuss a related term that I call the "means of control" or "control means."

SLIDE 3 - MEANS OF CONTROL

Whereas the term "control method" identifies WHAT parameter is being controlled, the "control means" speaks to HOW control is achieved from an engineering and facility operating perspective. Three basic means of control are shown in this slide and listed in the (general) order of preference from a criticality safety standpoint.

* **Passive engineered** - This means of control involves passive, fixed, design features or devices rather than moving parts. Human intervention is not required. This general class includes the use of fixed geometries and well as special passive devices such as an air brake device to prevent the backflow of solution. Advantage is taken of natural forces, such as gravity, rather than electrical or mechanical action.

This is generally regarded as the preferred means of control because it provides high reliability, protection against a broad class of potential criticality scenarios, and requires little operational support by facility personnel to maintain effectiveness.

* **Active engineered** - This means of control involves the use of add-on, active hardware (i.e., electrical, mechanical, hydraulic) that protect against criticality. These devices act by sensing a process variable important to criticality safety and providing automatic action to secure the system to a safe condition (i.e., no human intervention required). When passive engineered controls are not feasible, active engineered controls are an attractive alternative. However, all of these devices are subject to random failure and to human error occurring during operations and maintenance activities. Also, active engineered devices generally require a fairly considerable amount of support to maintain their effectiveness in terms of surveillances, periodic functional checks, preventive and corrective maintenance.

* **Administrative controls** - This means of control relies on the judgment, training, and responsibility of people for their implementation. These controls may be action or caution steps in an operating procedure or steps in a surveillance program. Because they are human based, and therefore subject to error in application, administrative controls are generally regarded as the least desirable means of control. In some instances, however, reliance must be placed on this means of control, at least in part. Purely administrative control may be augmented effectively by warning devices (visual or audible) which mandate operator action according to a procedure.

Before proceeding, some clarification may be needed regarding the distinction between administative control, as used here, and the other two control means. Obviously, all three basic means of control rely ultimately on administrative actions of some type (e.g., performing a functional test on an active engineered control or a periodic inspection of a passive engineered control. However, with administrative control, as used here, a human action is executed each time the control function is needed (e.g., a process sample requirement).

SLIDE 4 - CRITICALITY CONTROL METHODS AND EXAMPLES OF TYPICALLY ASSOCIATED CONTROL MEANS

For illustration, Slide 4 shows a typical association between a control method (i.e, what is controlled) and control means (i.e., how control is achieved). For example, geometry control is clearly passive engineered. Fissile concentration control is often implemented using both active engineered devices and administrative controls. Fissile mass control is usually implemented by purely administrative controls. (It is noted that the association shown on this slide is for illustration only).

The preferred control methods are those that can be implemented using the preferred control means (i.e., passive engineered over active engineered over administrative). During the design process, the most preferred control method(s) should be considered first for application and, then, successively falling back on the next preferred method, if the higher preferred method is not feasible.

Situations differ, and this discussion is not intended to provide hard and fast rules (i.e., one approach is always better than another). Rather, the intent is to stimulate thought aimed at making the best selections in each case, as suited to the particular circumstances.

SLIDE 5 - ITERATIVE DESIGN PROCESS

As is common to any design process, an iterative approach is required to arrive at a design concept that is both acceptable and optimized from a criticality safety standpoint. An illustration of a general iterative process is shown in Slide 5. For example, early-on in the design effort one might select certain control methods/means for examination and later discover some formidable problems. In which case, alternate control methods/means could be selected for consideration.

This slide shows a step labeled "Identify potential criticality scenarios." This step is important and is the subject of the next topic.

SLIDE 6 - IDENTIFICATION OF POTENTIAL CRITICALITY SCENARIOS

The first step in evaluating an element of risk is the recognition of it. Based on past experience, it can be expected that while many potential paths to a criticality event associated with a design concept will be obvious, other potential paths will not be apparent. For this discussion, a potential criticality scenario is defined as a credible pathway leading to the limit being exceeded for a controlled parameter. It is important to note that controls effective against one pathway MAY NOT be effective against another pathway.

Three factors contributing to successful identification of credible scenarios are shown in Slide 6. These are:

* Appropriate commitment of time and resources commensurate with the degree of complexity.

* Use of experienced personnel. These include criticality safety personnel and persons (operators/engineers/chemists) who have had operating experience in similar facilities.

* Use of systematic approaches. In many cases, potential accident scenarios may be postulated directly using previous operating experience, incident data, and engineering judgment. In complex situations, the use of systematic logic models may be helpful. These include for example: deductive logic tree analysis, inductive logic tree analysis, and Failure Modes and Effects Analysis (FEMA).

  An illustration of a deductive logic tree is shown in the next slide.

SLIDE 7 - EXAMPLE OF A DEDUCTIVE LOGIC TREE

As a first step, a careful survey should be made to identify all of the potential locations where criticality could occur. These would include, for example, process and storage vessels, cold feed tanks, sumps, ductwork, equipment holdup volumes, etc. For each such location, a review is made to identify the various credible pathways to criticality. Slide 7 shows an example of using a deductive logic tree for this purpose.

A deductive logic tree begins (at the top) with the identification of the controlled parameter(s). In the illustration in Slide 7, fissile concentration control is being considered as the the control method for Vessel 1 with the top event in the tree identified as, "high fissile material concentration." Next, the analyst chains backward in a logical, systematic way to identify all of the more basic events that could lead to the unsafe condition. In this case, a precipitation phenomena, an overconcentration phenomena, and an evaporation phenomena are identified for examination. In turn, the potential initiating events causing each of these phenomena are identified. Each such pathway is then reserved for study.

The next slide shows examples of potential phenomena and initiating events associated with the various control methods.

SLIDE 8 - EXAMPLES OF PHENOMENA AND INITIATING EVENTS LEADING TO EXCEEDING PARAMETER LIMITS
(2 parts)

Generally, the loss of control of a controlled parameter can result from several potential phenomena, as illustrated in this slide. For example, several potential phenomena are listed for exceeding fixed neutron poison limits (Slide 8, item 5), including: (1) leaching, (2) corrosion, and (3) loss from physical means (i.e., mechanical impact or fire). Situations differ, and not all of these phenomena are applicable in every case. None of the control methods is entirely immune from potential problems. For example, with geometry control (item 3), distortions of geometry may result from several potential phenomena, which should be considered.

This list is not intended to be an exhaustive. Rather, the purpose is to illustrate that there are generally multiple ways whereby parameter limits may be exceeded. The process of identify these pathways deserves special attention, including the involvment of experienced people. When the situation is complex (i.e., multiple pathways), the use of systematic approaches may be helpful.

SLIDE 9 - ACCEPTABILITY OF THE CONTROL SYSTEM

Protection against criticality requires a defense-in-depth approach such that no single failure can result in the potential for criticality. Consequently, if multiple scenarios (i.e., pathways) to criticality are identified, each such pathway should be protected through a defense-in-depth strategy.

Generally, it is best if protection can be provided through two independent parameters, such that criticality will not result if the specified limit is exceeded on any one parameter. However, for a large production facility processing plutonium or enriched uranium, this approach is not always practical, and reliance is placed on the control of a single parameter. In such cases, it is necessary to utilize multiple (at least two) controls on the same parameter. An example might be the combination of: (1) an administrative control in an operating procedure requiring that the fissile concentration level in a vessel be sampled and verified below certain limits before transfer, and (2) the presence of an active engineered control consisting of an in-line monitor to sense the fissile concentration level in the flow stream and automatically shut off stream flow, if a specified level is exceeded.

In all cases, it is important that the two protective functions are determined to be: (1) unlikely to fail, and (2) independent in terms of their failure modes

SLIDE 10 - DESIGNING TO FACILITATE LONG-TERM MANAGEMENT OF FACILITY OPERATIONS

Selections made during the design process will play an important role in the ability of facility operating personnel to successfully manage the criticality risks. Seven important considera-tion impacting manageability of the criticality risks are briefly described below:

* **Identifying controls important to safety** - Successful management of the criticality safety risks for a facility cannot be achieved without a clear understanding of the design features and control that are of key important to criticality safety. While many control features are obviously associated with criticality safety, some are not. This information must be documented as clearly as possible and transmitted from the design organization to the facility custodian.

* **Examining the manageability of the set of controls** - Every control feature will require some level of facility operational support to maintain a necessary high level of reliability, some control types requiring more support than others. Prior to finalizing the design, a review should be made of the entire set of controls from a facility-wide perspective to confirm that the total support level required is manageable.

* **Incorporating good human factors practices** - The use of good human factor practices in the design will greatly contribute to successful management of the criticality risks by reducing the potential for human errors in operations and maintenance. Considerations include the layout and labeling of controls, valves, and displays, and the physical space and arrangement, based on the notions of importance and frequency of use. It is essential that these considerations begin very early in the design process.

* **Incorporating uniformity into the design** - Incorporating uniformity (consistency) into the design will reduce complexity, training time, and the chances of human error. For example, the selection of criticality control methods/means for each of two unit operations in a facility that have similar processes and criticality considerations should be consistent, unless there is a compelling reason otherwise.

* **Designing to facilitate sampling** - For selected process and storage vessels, the ability to sample the solution in the vessel will be important to criticality safety. Where important, adequate provisions should be provided in the design to ensure that operating personnel can obtain samples that are representative of the vessel contents (e.g., proper location of sample points and the incorporation of mixing and recirculation capability).

* **Designing to facilitate inspections and cleanout** - For selected process areas and equipment, the ability of operating personnel to perform periodic inspections and cleanout will be important to criticality safety. This may include, for example, the periodic inspection of exhaust duct work, piping, and equipment for accumulations of solid fissile material. In the design process, this need should be recognized and appropriate design features incorporated (i.e., adequate space for inspections, viewing windows, access ports, etc.).

* **Designing to facilitate flushing** - In some cases, the ability to flush a line will be important to criticality safety. In those cases, the necessary provisions should be included in the design concept to permit an effective flushing operating (e.g., compatibility of flushing chemicals with materials of construction, selection of proper line sizes and slopes, adequate line support to limit sagging, incorporation of special valves needed for the flushing operation, and the proper locations of flush addition and exit points).

INTRODUCTION

- IT IS IMPORTANT THAT CRITICALITY SAFETY PLAY A MOJOR ROLE IN THE DESIGN PROCESS

  * Potential lethal doses to personnel

  * Substantial delays and shutdown to facility operations

- TOPICS

  ☐ Controlled parameters, control methods, and control means. (Slides 2, 3, 4)

  ☐ Iterative design process (Slide 5)

  ☐ Identification of potential criticality scenarios. (Slides 6, 7, 8)

  ☐ Acceptability of the control system (Slide 9).

  ☐ Designing to facilitate long-term management (Slide 10)

PROCESS PARAMETERS AND CONTROL METHODS

- Nuclear criticality safety is achieved by controlling one or more parameters of the system within critical limits (ANSI/ANS – 8.1).
- Controlled parameter. A parameter that is kept within specified limits (ANSI/ANS – 8.1)
- CONTROL METHODS
  - Geometry control
  - Spacing control (fixed equipment, rack design)
  - Fixed neutron poison control
  - Soluble neutron poison control
  - Fissile material concentration control
  - Moderation/reflection control
  - Fissile mass control
  - Enrichment control

MEANS OF CONTROL

- CONTROL "METHOD" – WHAT paramater is controlled
- CONTROL "MEANS" – HOW control is achieved (engineering/operating terms)
- THREE BASIC CONTROL MEANS
  * Passive engineered: Passive, fixed, w/o human action
  * Active engineered: Active, add–on, moving parts, w/o human action
  * Administative: Human action
- NOT EQUALLY PREFERRED

  Passive engineered best, active engineered next, administrative last.

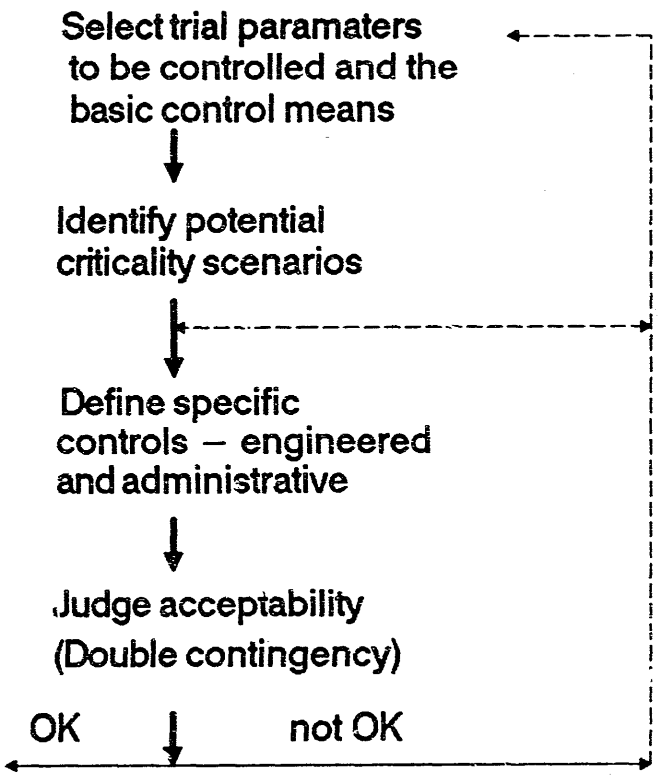
SLIDE 4

CRITICALITY CONTROL METHODS AND EXAMPLES OF TYPICALLY ASSOCIATED CONTROL MEANS

CONTROL METHOD	CONTROL MEANS		
(CONTROLLED PARAMETER)	PASSIVE ENGR.	ACTIVE ENGR.	ADMIN.
GEOMETRY	X		
SPACING (fixed equip, racks)	X		
FIXED NEUTRON POISON	X		
SOLUBLE NEUTRON POISON		X	X
FISSILE CONCENTRATION		X	X
MODERATION/REFLECTION		X	X
ENRICHMENT		X	X
FISSILE MASS			X

SLIDE 5

ILLUSTRATION OF ITERATIVE DESIGN PROCESS



Select trial paramaters to be controlled and the basic control means

Identify potential criticality scenarios

Define specific controls – engineered and administrative

Judge acceptability (Double contingency)

OK

not OK

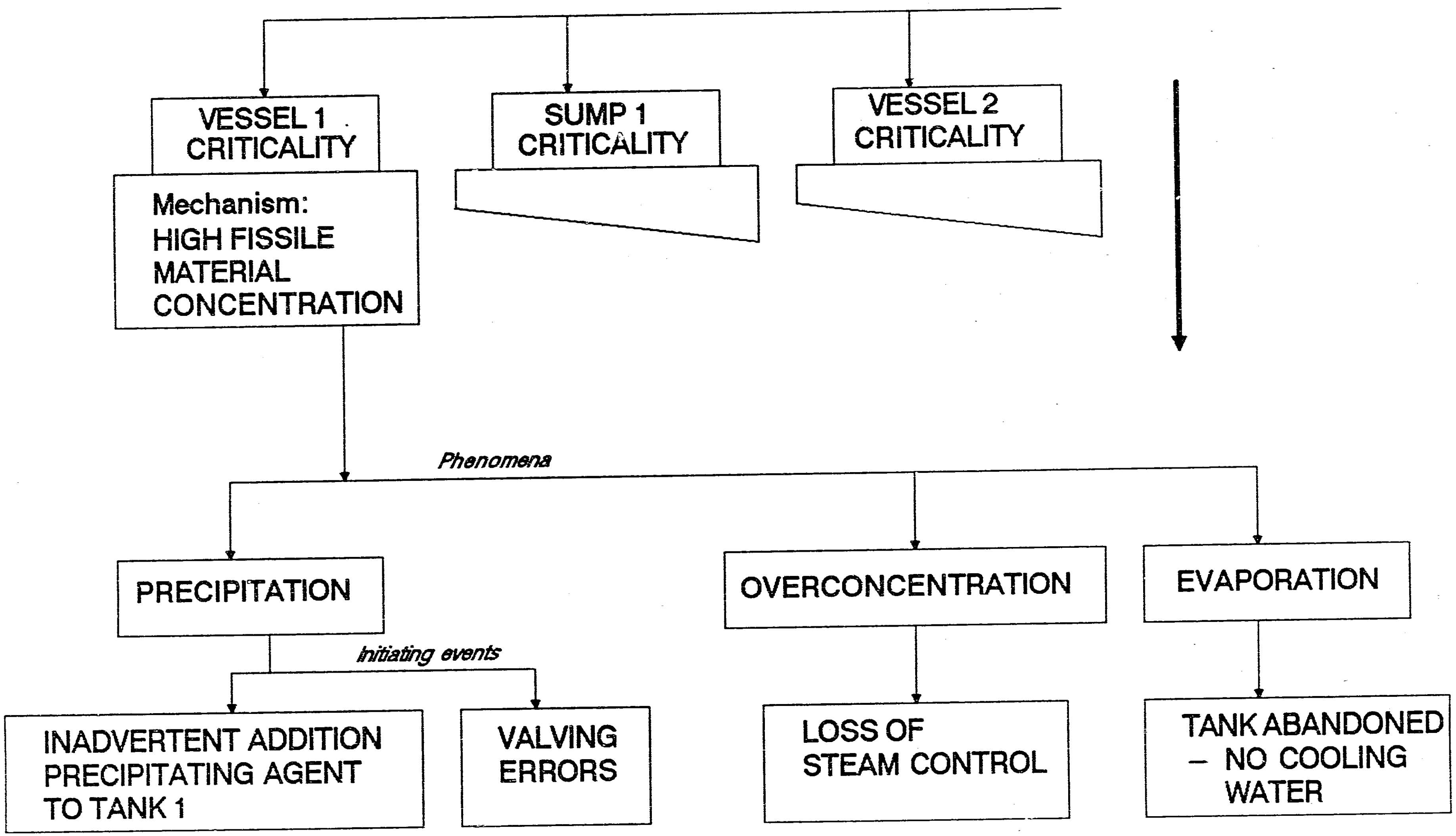
SLIDE 6

IDENTIFICATION OF POTENTIAL CRITICALITY SCENARIOS

- Potential criticality scenario – A credible pathway leading to the limit being exceeded for a controlled parameter.
- Controls effective against one pathway MAY NOT be effective against another pathway
- Factors contributing to successful identification.
  * Appropriate commitment of time and resources
  * Use of experienced personnel
  * Use of systematic approaches

SLIDE 7

EXAMPLE OF LOGIC TREE APPROACH



VESSEL 1 CRITICALITY

Mechanism: HIGH FISSILE MATERIAL CONCENTRATION

SUMP 1 CRITICALITY

VESSEL 2 CRITICALITY

Phenomena

PRECIPITATION

OVERCONCENTRATION

EVAPORATION

Initiating events

INADVERTENT ADDITION PRECIPITATING AGENT TO TANK 1

VALVING ERRORS

LOSS OF STEAM CONTROL

TANK ABANDONED – NO COOLING WATER

SLIDE 8 (1 OF 2)

EXAMPLES OF PHENOMENA AND INITIATING EVENTS LEADING TO EXCEEDING PARAMETER LIMITS

Mechanism	Examples—Phenomena: and Initiating Events
1. Fissile material concentration limits exceeded.	a. Precipitation: precipitant added inadvertently as a result of valving errors. b. Evaporation: tank abandoned with no cooling water. c. Solvent extraction: gradual accumulation of solvent material or large amount of solvent added to tank inadvertently. d. Overconcentration: loss of steam control.
2. Fissile material mass limits exceeded.	a. Double batching: human error. b. Fissile content higher than expected: incorrect sample result or misidentification. c. Slow accumulation: unrecognized slow leak.
3. Geometry specifications exceeded.	a. High internal pressure causing geometry distortions: eructation. b. Corrosion (thinning) of the vessel wall causing increase in internal vessel dimensions: loss of chemistry control.
4. Fissile material moderation limits exceeded.	a. Flooding of location designated to remain dry. Source - process liquids: backflow, leak, or spill. b. Flooding of location designated to remain dry. Source - sprinkler system water: location exposed for maintenance activities concurrent sprinkler operation. c. Moisture pickup from surrounding atmosphere: loss of control of cabinet atmosphere.

SLIDE 8 (2 OF 2)

EXAMPLES OF PHENOMENA AND INITIATING EVENTS LEADING TO EXCEEDING PARAMETER LIMITS

Mechanism	Examples--Phenomena: and Initiating Events
5. Fixed neutron poison specifications exceeded.	a. Leaching of poison material: inadvertent introduction of leaching materials. b. Corrosion of wall containing poison material: loss of chemistry control. c. Physical loss: fire or mechanical impact.
6. Soluble neutron poison specifications exceeded.	a. Improper chemical makeup: human errors in math and/or incorrect sample results. b. Precipitation of poison materials from solution: valving errors leading to introduction of precipitating agents. c. Dilution of soluble poison materials: valving errors introducing water (or other dilutants) or leaking across the tubes of a heat exchanger.
7. Neutron reflection requirements exceeded.	a. Excessive reflection from maintenance personnel: procedural violations.
8. Unplanned transport of fissile material to unfavorable geometry.	a. Leakage: from a vessel or line, through a closed valve, or across the tubes of a heat exchanger. b. Improper transport of process liquids: valving errors. c. Backflow: pressure upset - multiple initiating events. d. Backsiphonage: pressure upset - multiple causes. e. Liquid entrainment in an off-gas line: upset in operating conditions. f. An "air lift" phenomena: upset in operating conditions. g. Overflowing a vessel with the solution flowing through common vents to other units: loss of level control.

ACCEPTABILITY OF CONTROL SYSTEM

- DEFENSE – IN – DEPTH APPROACH
- NO SINGLE FAILURE CAN RESULT IN THE POTENTIAL FOR CRITICALITY
- BEST IF PROTECTED BY TWO INDEPENDENT PARAMETERS
- IF RELIANCE IS TO BE PLACED ON A SINGLE PARAMETER, NEED TWO INDEPENDENT MEANS OF PROTECTION (EACH UNLIKELY TO FAIL).

SLIDE 10

DESIGNING TO FACILITATE LONG–TERM MANAGEMENT OF FACILITY OPERATIONS

- IDENTIFYING CONTROLS IMPORTANT TO CRITICALITY SAFETY
- EXAMINING THE MANAGEABILITY OF THE SET OF CONTROLS (TOTAL FACILITY PERSPECTIVE)
- INCORPORATING GOOD HUMAN FACTORS PRACTICES
- INCORPORATING UNIFORMITY INTO THE DESIGN
- DESIGNING TO FACILITATE SAMPLING
- DESIGNING TO FACILITATE INSPECTIONS/CLEANOUT
- DESIGNING TO FACILITATE FLUSHING

END

DATE
FILMED

5/6/92