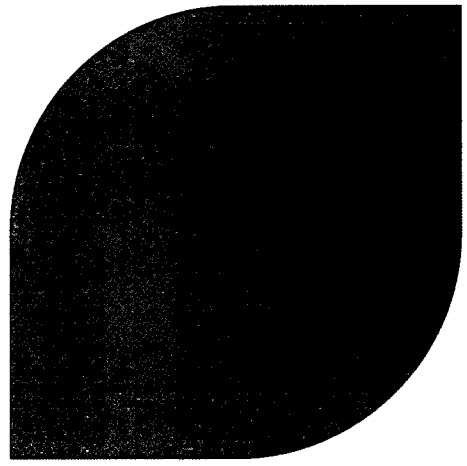


U.S. EPR Vital Area Identification

Pedro Salas
Randy Ford
Rockville, September 15, 2010

EPR™ by AREVA

AREVA

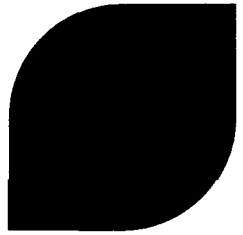
Agenda

- Objectives
- Regulatory Approach
- Comprehensive Technical Review
- Conclusions
- RAI No. 425 Closure Plan

Objectives

- Present to the NRC the regulatory basis AREVA used to identify the U.S. EPR Vital Equipment/Areas
- Identify a path for the resolution of the two FSAR Chapter 13 open items

RAI No. 425



- **RAI No. 425, Revision 1- [L]ist of vital equipment [must] include the following:**
  - *(U) The identification of vital equipment based on the nuclear power reactor plant design and the structures, systems, and components that have been designated as safety-related.*
  - *(U) Vital equipment includes all reactor designed SSCs providing safety functions that prevent or protect against the release of radioactive material that could endanger the public health and safety by exposure to radiation, as stated in 10 CFR 73.2.*
  - *(U) Vital equipment includes all reactor SSCs designed to function to prevent release of radioactive material that would exceed the radiological exposure stated in 10 CFR 52.47(a)(2), are identified as vital equipment. In addition, all safety-related SSCs that function to protect against radiological exposure exceeding the threshold of 10 CFR 52.47(a)(2), after the loss of SSCs that prevent the release of radioactive material, are also identified as vital equipment, in accordance with the 10 CFR 73.2.*
  - *(U) Vital equipment includes, in accordance with the 10 CFR 73.2, "any equipment, system, device, or material," for all modes of nuclear operations (i.e., power operations, hot stand-by, cold shutdown, refueling) is identified.*
  - *(U) Vital equipment includes all designed reactor SSCs in all redundant safety divisions that provide safety functions to prevent radiological release are identified as vital equipment.*
  - *(U) Vital equipment includes all equipment, systems, devices, or materials (i.e., supporting systems) that are relied on for control or motor forces (e.g., control systems, digital signals, electrical power, mechanical, compressed air, water, etc.) and function to prevent radiological release and protect against radiological exposure are identified as vital equipment (i.e., in accordance with the 10 CFR 73.2 definition that any equipment, system, device or material, the failure, destruction, or release of which could indirectly endanger public health and safety is vital equipment).*

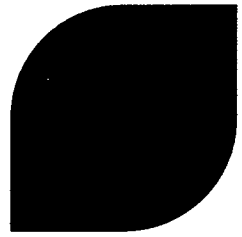
Regulatory Approach

- **Systematic and Deliberate Approach to the Identification of the U.S. EPR Vital Areas**
  - ◇ **Regulatory History of §73.2**
  - ◇ Identification of Published NRC Regulatory Guidance
  - ◇ Identification of Regulatory Precedent
  - ◇ NRC Response to Vital Area Designation after 9/11 (Operating Fleet Operating Experience)
  - ◇ NRC Public Meetings to Obtain NRC Clarification
  - ◇ Evaluation of Contemporary Technical Studies to Assess Consistency With Published NRC Guidance

Regulatory History of §73.2

- **On December 28, 1973 NRC Published 10 CFR 73 – Physical Protection of Plant and Materials**
  - *§73.2(h) – "Vital area" means any area which contains vital equipment within a structure, the walls, roof, and floor of which constitute physical barriers of construction at least as substantial as walls as described in paragraph (f)(2) of this section. [1973]*
    - *Vital area means any area which contains vital equipment. [2010]*
  - *§73.2 (i) - "Vital equipment" means any equipment, system, device, or material, the failure, destruction, or release of which could directly or indirectly endanger the public health and safety by exposure to radiation. Equipment or systems which would be required to function to protect public health and safety following such failure, destruction, or release are also considered to be vital. [1973 & 2010]*
- **§73.2 has been amended multiple times, but §73.2 (i) Remains Un-amended Since First Codified in 1973**

Published Regulatory Guidance



- **The NRC Has Published Three Regulatory Guidance Documents for the Identification of Vital Areas**

  - **January 23, 1978**
    - Definition of Vital Areas, Revision 1 – Review Guideline No. 17
  - **May 1983**
    - NUREG—0992 - Report to the Committee to Review Safeguards Requirements at Power Reactors [One of five findings related to vital areas]
  - **February 1988**
    - NUREG-1178 – Vital Equipment/Area Guidelines Study: Vital Area Committee Report

Published Regulatory Guidance

- **Definition of Vital Areas, Revision 1 – Review Guideline No. 17 (1978)**
  - **Review Guideline 17 has been the basis for NRC review of vital area identification**

Definition of Vital Areas, Revision 1 – Review Guideline No. 17 (1978)

▶ Assumption and Definitions

◇ **To "endanger the public health and safety by exposure to radiation" requires a significant off-site release of radioactivity. For LWR's the following sources of significant quantities of radioactivity should be considered:**

a. The reactor core,

b. Spent fuel,

c. Radwaste systems, if the total radwaste inventory is greater than nxC, where:

- n is the ratio of the applicable dose guideline of 10 CFR 100 to the dose computed for accidental releases in Chapter 15 of the FSAR, and
- C is the release (curies) assumed in the accidental release calculation of the FSAR

Definition of Vital Areas, Revision 1 – Review Guideline No. 17 (1978)

▶ Assumption and Definitions

◇ Vital Areas fall into two general categories:

a. Type I vital areas, i.e., those areas wherein successful sabotage can be accomplished by compromising or destroying the vital systems or components located within this area. (By definition, an area containing systems or components whose failure or destruction results in a direct release is a Type I vital area.)

...Because there was no regulatory basis for requiring an additional level of protection for Type I areas, no practical use was made of this distinction. NUREG-178, Section 3

b. Type II vital areas, i.e., those areas which contain systems or components whose failure or destruction would lead to successful sabotage only in conjuction with additional sabotage activity in at least one other, separate vital area. (Safety related equipment designed to mitigate the consequences of failures of other systems usually falls into this category.)

◇ When classifying vital equipment as Type I or II, the following assumptions apply:

a. The concurrence of violent natural phenomena with a security contingency need not be considered.

b. Random (accidental) failure of equipment concurrent with a security contingency need not be considered. However, a security contingency during routine or planned outages of equipment, as permitted by technical specifications, must be considered.

c. Loss of off-site power must be assumed since it is impractical to protect transmission lines against sabotage

Definition of Vital Areas, Revision 1 – Review Guideline No. 17 (1978)

▶ Assumption and Definitions

◇ Discussion

- The definition of vital equipment, 73.2 (i), includes equipment whose failure would lead to a direct release, as well as equipment required to function for the protection of public health and safety following a postulated attack. This is analagous to the definition of safety-related equipment, which includes primary fission product barriers, as well as the systems required to mitigate the consequences of a breach of the barrier. Therefore, essentially all safety related equipment must be considered vital. In order to avoid duplication of safety analyses, the systems listed in Reg. Guide 1.29 should be considered vital.

- It should be noted that a facility which provides sufficient delay time to permit interruption of external threat of §(a)(1) at all vital area barriers, and for which adequate protection against insider threat of §(a)(2) is provided for all vital areas would meet the requirements of 73.55 without the designation of any Type I Vital Areas. In practice, however, it is to licensee's advantage to segregate vital areas into Type I and II, in order to take credit for the fact that a saboteur could not achieve successful sabotage in Type II vital areas without penetrating additional barriers.

Published Regulatory Guidance

▶ NUREG-0992 - Report to the Committee to Review Safeguards Requirements at Power Reactors

◇ Findings:

2. Impact of Vital Area Access Controls on Safe Operation of Facilities

The degree of internal compartmentalization for security purposes (vital areas), can adversely affect operational safety. This is true, specifically during abnormal or emergency situations, if operational personnel do not have keys or other methods for gaining prompt access to all plant areas in the event of a failure of the normal card key access system. The number of vital areas varies significantly among licensed plants from a minimum of three at some, to over thirty at others. Doors and equipment which are locked for other purposes such as radiation protection, and administrative control present a similar potential for safety impact.

Published Regulatory Guidance

- **NUREG-1178 Vital Equipment/Area Guidelines Study: Vital Area Committee Report, Final Report, February 1988**
  - ◇ On May 1, 1985, the NRC EDO directed the staff to initiate a study to re-evaluate the existing guidelines and bases used to determine what are the vital equipment and areas to be protected against radiological sabotage
  - ◇ The Vital Area Committee recommended that the proposed vital equipment/area protection philosophy and analysis assumptions presented in section 6.1 of NUREG-1178 be adopted and implemented
  - ◇ The Vital Area Committee reported that satisfaction of the requirements and assumptions of Review Guide 17 continues to be acceptable as an alternative to NUREG-1178
  - ◇ The committee stated that the assumptions represent a comprehensive and consistent approach to determining equipment and areas to be designated as vital and that their application will contribute to the overall program designed to provide a high degree of assurance against radiological sabotage
  - ◇ The committee also stated that these assumptions were consistent with existing regulations. §73.2(i) remains un-amended to date

Published Regulatory Guidance

▶ NUREG-1178 Vital Equipment/Area Guidelines Study: Vital Area Committee Report, Final Report, February 1988

◇ James M. Taylor, Director, Office of Inspection and Enforcement concluded that NUREG-1178 assumptions conform with the requirements of §73.2 that define vital equipment

- December 5, 1985 Memorandum; James M. Taylor, Director, Office of Inspection and Enforcement to Frank J. Miraglia, Chairman, Vital Area Committee

A. *Rulemaking*

No change in the rules is necessary to implement the assumptions because the definition of vital equipment now contained in 10 CFR 73.2(i) is broad enough to include the equipment that may be designated as vital under the Committee's assumptions. *The very broad terms of the definition allow essentially any safety-related equipment or systems to be designated as vital. The Committee's assumptions fall within the scope of the current definition and protection of vital equipment based upon them would satisfy the standards of 10 CFR 73.55 and be acceptable.*

Published Regulatory Guidance

▶ NUREG-1178 (1988) - Key Assumptions:

1. *For purposes of protection against radiological sabotage, the primary coolant pressure boundary consists of the reactor vessel and reactor coolant piping up to and including a single, protected, normally closed isolation valve or protected valve capable of closure in interfacing systems.*
2. *Any transient or event that causes significant core damage will result in an attendant 10 CFR 100 release.*
3. *One train of equipment (with the associated piping, water sources, power supplies, controls, and instrumentation) that provides the capability to perform the functions (reactivity control, decay heat removal, and process monitoring) that are necessay to achieve and maintain hot shutdown for 8 hours from the time of reactor trip should be protected as vital. In addition, the major components of the reactor coolant make up system and associated support equipment necessary to achieve this goal should be protected as vital.*
4. *The control room and any remote locations from which vital equipment can be controlled or disabled (such as remote shutdown panels, motor control centers, circuit breakers, or local control stations) should be protected as vital areas.*
5. *Only the power mode of reactor operation and hot standby (for PWRs) need be considered as long as all equipment designated as vital for power operation is maintained as vital in other modes.*

Published Regulatory Guidance

NUREG-1178 (1988) - Key Assumptions (Continued):

6. *Off-site power is unavailable.*
7. *Random failures do not occur simultaneously with an act of radiological sabotage. However, the saboteur can take advantage of the unavailability of equipment during maintenance. Thus, whenever any components or systems normally protected as vital are inoperable for any period of time, appropriate compensatory measures (such as stationing guards at alternate 1ocations) must be taken to ensure that the capability to reach hot shutdown is maintained.*
8. *Breaks in multiple main steam lines that cannot be isolated lead to 10 CFR 100 releases.*
9. *Cable runs in trays and conduit need not be protected as vital unless cables necessary for safe shutdown capability are individually identifiable and the identification is reasonably accessible. However, cable terminals or junctions and areas such as cable spreading rooms, through which large numbers of cables pass, must be protected.*
10. *Saboteurs may use explosives in amounts that they can carry.*
11. *No credit is given for equipment not located in vital areas.*
12. *Following the start of a refueling outage, the spent fuel pool should be protected as vital long enough to ensure that sabotage to the pool cannot result in a 10 CFR 100 release.*
13. *The backup supporting power supply of the Central Alarm Station (CAS) is essential for continuous operation of CAS in the event of loss of normal power.*

Regulatory Precedent

- **NRC Safety Evaluation Reports for Physical Security Plans Reviewed Per Review Guide 17 Unavailable to the Public Due to SGI Considerations**

- **July 1994 - NUREG-1503, "Final Safety Evaluation Report Related to the Certification of the Advanced Boiling Water Reactor Design, Main Report"**

Regulatory Precedent

- **NUREG-1503, "Final Safety Evaluation Report Related to the Certification of the Advanced Boiling Water Reactor Design, Main Report,"**
  - ***13.6.3.3 Vital Areas***

    ... The staff is satisfied that the list of vital equipment includes all active and passive plant equipment essential to safe shutdown of the reactor, including necessary support systems, the reactor vessel and the remainder of the reactor coolant system pressure boundary within the primary containment, the suppression pool, spent fuel in the fuel pool, and any associated piping, equipment, and controls whose failure could result in an offsite release in excess of 10 CFR Part 100 limits. The staff finds this to be compatible with NRC Review Guideline 17 (January 23, 1978, memorandum from R. Clark to safeguards licensing staff). Prior to issuance of a COL, the staff's review of the designation of equipment as vital in plant-specific applications will focus on plant support equipment outside the scope of the certified ABWR design.

    In addition, 10 CFR 73.55(e) requires that the central alarm station be considered a vital area and secondary power supply system for alarm annunciator equipment and that non-portable communications equipment be located in vital areas. The secondary alarm station also is typically on site and treated as a vital area. Vital area classification of the central and secondary alarm stations was identified as DFSER COL Action Item 13.6.3.3-1. In SSAR Amendment 25, GE stated in Section 13.6.3.8 that the COL applicant will provide site-specific security, contingency, and guard training plans... Vital area classification will be addressed at the time of the plant-specific security plan review. The staff finds it to be acceptable.

Regulatory Precedent

▶ NUREG-1503 - Question 910.11

- ◇ *Submit the analysis that supports the vital areas results described in this section. Affirm that these areas include all or the reactor coolant pressure boundary, including appropriate motor control centers and power supplies, and systems required for mitigation of transients, and support systems (e.g.,. cooling water, instrumentation, control power) necessary for these systems to operate. Describe which systems arc included in paragraph (l)(a) of Section 13.6.3.3 as vital "core cooling systems," and which components in these system are vital components. Which vital systems would be out of the scope of the standard Nuclear Island and thus subject to plant specific review (13.6.3.3)*
- ◇ *RESPONSE 910.11*

  Response to this question is provided in revised Subsection 13.6.3.3.

NRC Response to Vital Area Designations after 9/11

- **NRC Has not Alerted Licensees/Applicants that Post September 11, 2001 Vital Area Related Guidance Documents are Considered Inadequate; nor has NRC Published Alternate Criteria Affecting Vital Areas/Equipment Identification**
  - ◇ **B.5.b Orders Were Silent on the Topic**
  - ◇ **The 2008 Revised Security Rule Was Silent on the Topic**
  - ◇ **Licensees Were not Asked to Reassess Their Vital Equipment Lists**

NRC Public Meetings

▶ SECY-08-0099 - FINAL RULEMAKING - POWER REACTOR SECURITY REQUIREMENTS

◇ Integrated Comment Responses Supporting Final Rule: Power Reactor Security Requirements

- ***Comment Summary:***
  *A commenter at the **November 15, 2006 public meeting** asked if a NUREG from the 19[8]0s is a good source for defining vital equipment.*

- ***NRC Response:***
  NRC published information remains acceptable unless otherwise stated by the Commission.

NRC Public Meetings

▶ SECY-08-0099 - FINAL RULEMAKING - POWER REACTOR SECURITY REQUIREMENTS

◇ Integrated Comment Responses Supporting Final Rule: Power Reactor Security Requirements

- ***Comment Summary:***
  *One commenter at the **November 15, 2006, public meeting** asked for a clarification of the relationship between target sets and vital equipment. The NRC responded that the difference between vital equipment and target sets would be that target sets include vital equipment, but vital equipment does not always contain everything that may be part of a target set. Target sets would be the combination of equipment, systems, even personnel, that would need to be disabled or destroyed in order to cause a problem. So, the commenter deduced that vital equipment would be part of the target set, but the target set, itself, may include additional things to it that would also be protected.*
  The NRC explained that requiring licensees to protect target sets protects those systems, personnel, or equipment that are necessary for a safe shutdown. The NRC concluded that vital equipment is related to safe shutdown and target sets are related to release. Another commenter at the November 29, 2006, public meeting asked if a licensee can lose vital equipment without either losing the ability for safe shutdown or losing a target set. The NRC responded that yes, it is possible.

- ***NRC Response:***
  Vital equipment is related to safe shutdown while target sets are related to release of radioactive material (or significant core damage and spent fuel sabotage). Therefore, the physical protection program design criteria in 10 CFR 73.55(b) focuses on prevention of significant core damage and spent fuel sabotage and the ability to effectively implement the protective strategy as performance-criteria resulting from the protection of target sets.

RAI No. 425 vs Contemporary Technical Studies

- **Sandia Report (SAND2008-5644), September, 2008 - Vital Area Identification for U.S. Nuclear Regulatory Commission Nuclear Power Reactor Licensees and New Reactor Applicants**
  - ◇ **ACKNOWLEDGEMENTS** The authors would like to acknowledge the support of the NRC, in particular, Albert Tardiff, for helping to produce this document.
  - ◇ ***1.2 Purpose***

    The purpose of this document is to describe a structured process that can be used to identify the areas of a nuclear power plant that should be designated as vital areas. The set of vital areas identified using this process should be provided with the protection measures specified in 10 CFR 73.55 to reduce the risk of radiological sabotage. The vital area identification process is based on the information contained in the following documents:

    - ***NUREG-1178 (Vital Equipment/Area Guidelines Study: Vital Area Committee Report) [Ref.6],***
    - ***Draft IAEA-NUCLEAR SECURITY SERIES-XXXX (Identification of Vital Areas at Nuclear Facilities) [Ref. 8]***
    - ***SAND2004-2866 (A Systematic Method for Identifying Vital Areas at Complex Nuclear Facilities) [Ref. 9],***
    - ***NUREG/CR-0809 (Fault Tree Analysis for Vital Area Identification) [Ref. 4], and***
    - ***Nuclear Power Plant Security Assessment Format and Content Guide [Ref. 10].***

RAI No. 425 vs Contemporary Technical Studies

- **Sandia Report (SAND2008-5644), September, 2008 - Vital Area Identification for U.S. Nuclear Regulatory Commission Nuclear Power Reactor Licensees and New Reactor Applicants**
- **Vital Area Identification Assumptions**

1. *In order to prevent radiological sabotage of a nuclear power plant it is necessary to prevent significant core damage and spent fuel sabotage. Vital areas should be identified so as to protect a minimum set of the systems, personnel, and equipment needed to prevent significant core damage and spent fuel sabotage. The radiological sabotage criterion for inventories of material other than the reactor core and the spent fuel pool is a release of radioactive material in excess of 10 CFR Part 100[Ref. 11] limits. A minimum set of equipment needed to prevent releases in excess of Part 100 limits from inventories of radioactive material other than the core and the spent fuel pool must also be protected in vital areas.*
2. *All distinct operating states (power operation, hot standby, cold standby, and refueling) must be addressed in the vital area identification process. Different operational states may rely on different equipment to perform safety functions and may require protection of different areas to ensure protection against sabotage. A set of vital areas may be identified for each operational state or a bounding set of vital areas that provides protection during all operating states can be selected. The latter approach may be advantageous from a physical protection standpoint to minimize or eliminate the need for reconfiguring physical protection measures when the operational states change.*
3. *In building logic models for the VAI analysis, it is not necessary to assume that a vital equipment maintenance outage occurs concurrently with an attack. Vital equipment maintenance outages that occur during operations should be addressed as specified in Reference 10, Volume 3 and may require the implementation of compensatory measures such as designating and protecting alternate vital areas containing redundant equipment.*

RAI No. 425 vs Contemporary Technical Studies

Vital Area Identification Assumptions

4. *It is not necessary to assume that a random failure of vital equipment occurs concurrently with an attack.*
5. *Credit can be taken for operator actions if all of the following conditions are met:*
    4. *There is sufficient time to implement the actions between the sabotage act(s) and the onset of core damage or spent fuel melting.*
    5. *Environmental conditions in the area where the actions must be performed allow access of personnel.*
    6. *Adversary interference with the completion of the actions is precluded.*
    7. *Any equipment needed to complete the actions is available and ready for use.(This may require that the equipment is secured in a vital area.)*
    8. *Approved procedures for the actions exist.*
    9. *Training is conducted on the procedures covering the actions under conditions similar to the scenarios for which the actions are credited.*
6. *Spurious actuation of equipment (as might occur as a result of fire) must be addressed.*
7. *The effects of cyber attacks on equipment performance must be addressed.*
8. *The inability of an adversary to identify cable trays containing power or control cables should not be used as a criterion to remove the cable trays from the vital area identification process if cutting the cables would disable the equipment to which the cables are connected.*
9. *Loss of coolant incidents and main steam line breaks must be considered credible adversary acts unless access to all locations from which such acts could be performed are inaccessible because of disabling radiation levels or environmental conditions so severe that an attacker would not be able to carry out the required acts before being incapacitated.*
10. *Assume that loss of offsite power occurs concurrent with an attack.*
11. *Assume that all equipment outside the protected area of the plant is lost unless continued operation of the equipment makes the situation worse.*

Comprehensive Technical Review

- The U.S. EPR Vital Area Identification starts with the NUREG-1178 Assumptions, but exceeds the minimum requirements
- The U.S. EPR design includes equipment not required by NRC guidance documents but deemed prudent
- The U.S. EPR design uses compartmentalization to improve the security protection
- Very little gap between the U.S. EPR design and the most conservative NRC interpretation of the requirements

Conclusions

- AREVA has approached the identification of the U.S. EPR vital areas with a prudent regulatory approach
- The U.S. EPR exceeds the minimum requirements stipulated in published NRC guidance documents

RAI No. 425 Closure Plan

- AREVA requests NRC to consider this discussion and provide feedback by October 1
- AREVA will respond to open items (RAI 425) by October 28
- At the ACRS meeting on FSAR Chapter 13 (Nov 2) NRC and AREVA should be able to identify the resolution pathway


AREVA