TRW

I 44 f- mtbk - issues

1 March 1977

Mr. L. J. Evans
Chief, Requirements Analysis Branch
Nuclear Regulatory Commission
Room 850
7915 Eastern Avenue
Silver Springs, MD. 20555

Dear Mr. Evans:

Enclosed are some of our preliminary thoughts for an Appendix to 10CFR73 dealing with Quality Assurance for Safeguard Systems.

Sincerely yours,

Harvey J. Spiro

Harvey J. Spiro

HJS:cs

Enclosure

ENERGY SYSTEMS GROUP • TRW INC • WESTGATE PARK • 7600 COLSHIRE DRIVE, McLEAN, VIRGINIA 22101 • (703) 893-2000

PURPOSE OF QA FOR SG SYSTEMS: Assure that equipment and systems installed to safeguard SNM: (1) Meet or exceed design specifications at all times; (2) Prevent any compromise of the integrity of SNM; and (3) Provide immediate and obvious indication and/or notification of incipient failure.

ORGANIZATION: Adequate staff with authority and resources to maintain the SG system at design specifications at all times, and to restore any aspect of SG system to full design specifications immediately upon discovery of any subsystem failure. As a minimum, the organization must accomplish the following:

- Initial Installation - All safeguards hardware and systems must be tested to meet design specifications at time of installation
- Replacement Components - All replacements must be tested to meet design specifications at time of replacement
- Preventive Maintenance - A program of PM must be effected, providing regularly scheduled inspection and repairs. These must be sufficiently thorough and frequent to prevent incipient problems resulting from gradual degradation of SG systems.
- Continuous Monitoring - Licensee must assure that key SG system components are continuously monitored for operational status, and must provide for immediate notification of and response to failure of any such component. Key safeguards systems are those whose failure could result in an unacceptable compromise of the integrity of SNM.

- Can these be stated in perf. terms? functions why we desire to be accomplished?

INTEGRATION OF SYSTEMS: Licensee must demonstrate that components of all systems not only work separately but also work when integrated into overall SG systems.

? ? functions?

STANDBY SYSTEMS: Licensee must provide adequate standby systems to assure that SNM does not become vulnerable to theft or diversion at any time.

SPECIFICATION 1.0 The licensee should be required to establish and describe in detail a system for the prevention of the illicit removal of SSNM from the plant site .

Specification 1.1 The licensee should be required to establish and describe in detail a system for the prevention of the illicit removal of SSNM from process streams, storage and laboratory activities. In establishing such a system the licensee should provide methods for

(1) Minimizing the number of persons authorized access to MAAs,

(2) Maximizing the level of trust and reliability of persons so authorized,

(3) Minimizing the number of points in the process and equipment for the ready removal of SSNM and minimizing the number of points where the authorized removal of SSNM is necessary,

(4) Verifying the authorizations and instructions for removal of SSNM (samples or bulk material) prior to such removal,

(5) Promptly verifying that SSNM which is removed is received by intended receivers,

(6) Verifying that at least two persons are present in each area of a MAA when occupied or that the activities in the area are otherwise observed at all times when occupied, and that the MAA has an active intrusion detection device (and alarm) in operation when it is unoccupied,

(7) The control of SSNM by procedures which specify the point or points in the process, etc. that SSNM may be introduced or removed, methods of handling of removed SSNM while outside of process etc. equipment but still within the MAA and the authorization procedures and recordkeeping requirements for SSNM additions or removals,

(8) Protecting SSNM from theft or diversion during non-routine operations and emergency situations (including maintenance of or alteration to facilities, criticality, fire, natural phenomena, injury to persons within the MAA, inspections and visits, or other attention attracting or process interrupting situations),

(9) Tamper-safing of containers of SSNM which is not in process and of storage vaults,

(10) Training, retraining and testing of operating personnel, guards and escorts in -

(a) the recognition of the existence of illicit materials or items which could be used to further the diversion of SSNM,

(b) the recognition of illicit activities within a MAA,

(c) the prompt reporting of the presence of illicit materials or items and activities,

(d) procedures to be followed to protect SSNM from diversion during non-routine operations and emergency situations.

SPECIFICATION 1.2 The licensee should be required to establish and describe in detail a system for the prevention of the illicit removal of SSNM from material access or item control areas.

Specification 1.2.1 The licensee should be required to establish and describe in detail a system for the prevention of the illicit removal of SSNM from a material access or item control area for each individual access point in the physical barrier to the area. In establishing such a system a licensee should provide methods for;

(1) Searching all persons exiting a MAA for SSNM, shielded or unshielded, concealed or unconcealed, in articles of clothing or in or on the body, including a description of the search methods used at each routine egress point of the MAA.

(2) Searching all packages and articles (including waste packages) exiting a MAA for SSNM, including a description of the search methods used to uncover shielded or unshielded SSNM contained in false compartments, hollowed out articles, equipment items and miscellaneous containers.

(3) Minimizing the numbers and types of packages and articles to be removed from the MAA.

(4) Verifying the contents of all SSNM containers at time of loading and tamper-safing thereof.

(5) Reconciling of SSNM container identification and seal numbers with transfer papers prior to release from MAA.

(6) Verifying the authorization for removal of SSNM from a MAA prior to release therefrom.

(7) Verifying the authorization of individuals accompanying a removal of SSNM from a MAA.

(8) Minimizing the number of points in the MAA barrier where the authorized removal of SSNM is permitted.

(9) Searching all vehicles exiting a MAA for unauthorized removal of SSNM, including a description of the search methods used and the extent of each search. The licensee should specify search procedures for every type of vehicle utilized at the SNM removal point to include product vehicles, spent fuel

cask vehicles, vehicles transporting special supplies or equipment, and vehicles transporting waste products and scrap.

(10) Prevention of any removal of SSNM from a MAA by authorized transfer or otherwise during the existence of emergency conditions on the plant site (including attack, suspected theft of SSNM, criticality, fire, natural phenomena, injury to persons or other attention-attracting situations).

(11) Prevention of removal of SSNM through MAA egress points which are not specifically authorized for SSNM removal.

(12) Remote surveillance of MAA egress points for personnel, vehicles, packages, equipment and other aritcles, and SSNM containers.

(13) Training, retraining and testing of guards and watchpersons in -

(a) recognition of SSNM and possible containers which could be used for illicit removal thereof,

(b) thorough search procedures for personnel, vehicles and packages,

(c) authorization procedures for SSNM container removal,

(d) authorization verification procedures.

(e) reaction to emergency situations to prevent removal of SSNM from the MAA.

Specification 1.2.2 The licensee should be required to establish and describe in detail a system for the prevention of the illicit removal of SSNM from a material access or vital area through the physical barrier to the area. In establishing such a system a licensee should provide methods for:

(1) Hardening the physical barrier to prevent penetration thereof.

(2) Blocking of existing openings in the physical barrier to the passage of items which could contain SSNM (including windows, pipe penetrations, ventilation ducts, sewage lines, waste lines, etc)

(3) Determining that pipelines and conduits in the physical barrier do not contain SSNM.

(4) Monitoring the physical barrier for the detection of drilling, sawing, explosion or puncturing activities which could result in a breach in the integrity of the barrier or damage to blocking mechanisms set forth in (2) above.

I 46 — f - W.G. mtg. - issue papers

3/3

Andy — This is helpful — it would be even better if each page's entries corresponded (same order + lang. type — e.g. "Control of access" on Bldr. pg = "provide a MAA perimeter + access control" on your pg.) We may have to use this eventually —
Be

DRAFT
ASPoltorak
3/3/77

DISCUSSION OF BASIC CAPABILITIES

Gross Statement of Basic Capabilities

1. Control of Access
2. Control of Activities and Conditions of Access
3. Control of removal from SNM access areas
4. Control of breaches of containment
5. Control intruders

Definition

Control implies the establishment of authorization, detection and response.

Strict interpretation of the Builder concepts:

1.) Prevent unauthorized persons, material, and vehicles from entering MAAs

2.) Prevent unauthorized activities from taking place within MAA and VA, and detect and correct unauthorized conditions of access (personnel situations)

3.) Prevent unauthorized removal of material from MAAs

4.) Detect and correct holes in physical containment structures (an apparent QA function)

5.) Detect and engage the external bad guys.

Poltorak View - don't rely heavily on the words of the Builder capabilities, relate to perimeter, area, defense-in-depth concept.

a) provide a PA perimeter, access control and access penetration detection

b) provide for activity control (surveillance) in PA

c) provide a MAA perimeter and access control (all SNM is to be within MAA for storage and processing, and leave only for authorized removal from site or between MAA's ?)

d) provide removal control of SNM at MAA perimeter

e) provide MAA perimeter penetration control

f) provide for control over activities and conditions within MAA which are unauthorized to the extent of making SNM vulnerable (possibly with special control within more defined areas)

g) provide for control or containment of SNM within MAA, defining quantity and location (link with material accounting) and protection, potentially increasing in intensity as desirability of SNM increases.

Connect into system spec's

Translation into Basic Capabilities

1) Protect against unauthorized penetration of PA.

2) Prevent unauthorized access to MAA

3) Prevent unauthorized removal of SNM from MAA

4) Detect and correct unauthorized activities and conditions

5) ~~Assure containment or control is provided for SNM within MAA~~ Prevent unauthd movement of SNM w/in MAA

Jones Views

✓ 1) Extend access control to include PA and all barriers and/or containment around SNM

2) Watch what the people are doing and .... ?

✓ 3) Extend removal control to include all barriers and/or containment around SNM and any movement of SNM within any containment.

4) Look for holes in the physical containment structure, a QA function.

5) Stop the outside threat.

Still have not identified the number or function of containment

& he won't because he hasn't decided why it should achieve

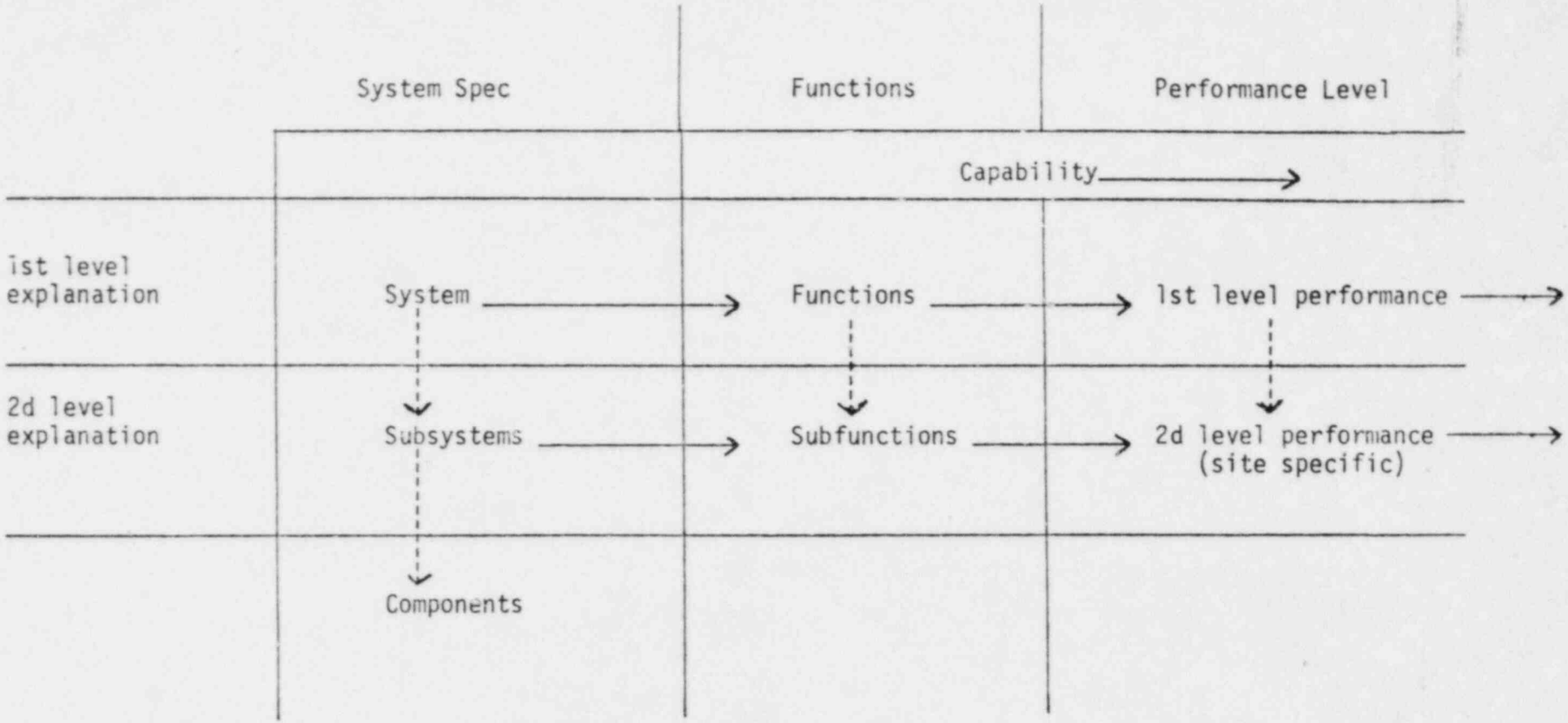
f – Hbk – Issue Paper

SA1 Assessment Briefing

- State must do <u>both</u> <u>vulnerability</u> analysis + <u>probability</u> analysis
  - use experts (qualitative) to say have no <u>vulnerability</u>
  - if ~~Experts~~ say no vulnerability then use <u>probability</u> analysis to determ S/C level

- could analogize to why include essential system spec. in Upgrade Rule
  - they assume no major vulnerability

STRUCTURE OF CAPABILITY SECTION OF UPGRADE RULE



TRW 2/18/77 I 49

OPTION PAPER: QA AND CONDITIONS

PURPOSE

This paper discusses the way in which the meaning of "conditions" in Basic Capability 2 might be influenced by decisions made with regard to Quality Assurance.

QUALITY ASSURANCE OPTIONS

1. Elevate QA to the level of a Basic Capability. This could be accomplished if we define "conditions" in a manner that includes any physical object which influences the performance of the safeguards system including the system itself. Then the requirement to prevent unauthorized conditions effectively means to prevent any degradation of expected safeguards performance - clearly a QA capability.

- Advantages
  - Emphasizes the need for licensees to assure that the functioning of safeguards systems meets design expectations.
  - All things which might degrade the designed safeguards performance are explicitly addressed.
- Disadvantages
  - The QA requirement and an activities requirement are grouped in BC2 in an awkward manner. This, of course, could be resolved by making QA a separate Capability.
  - QA for fuel reprocessing plants is dealt with elsewhere in a generic manner (Appendix B to 10CFR Part 50). It may be unnecessary and excessive to restate this in a Basic Capability.
  - Logical consistency becomes a problem. (See paragraph 2 below.)

2. Treat all QA as a constraint. This removes QA from the Basic Capabilities entirely except as the "no degradation of performance" constraint applies to all Capabilities.

- Advantages
  - All things which might degrade the designed safeguards performance are explicitly addressed.
  - The logical consistency of the performance rule is strengthened. This is because QA is not really a Capability vis á vis potential adversaries, but rather a factor which enables the capabilities to be maintained once they are achieved.
  - The precedent set by Appendix B to 10CFR50 is maintained.
- Disadvantages
  - It may be argued that safeguards QA is not sufficiently emphasized if it is stated outside a Basic Capability.

3. Taking QA as a constraint, have this requirement apply only to the safeguards system.

- Advantages
  - Logical consistency is strengthened as in Option 2.
- Disadvantages
  - This statement of QA ignores those aspects of the plant and its equipment which directly influence the performance of the safeguards system, yet which are not a part of that system.

4. Apply QA as a constraint to safeguards systems, but apply it as a capability to conditions which influence the performance of safeguards systems.

- Advantages
  - All things which might degrade the designed safeguards performance are explicitly addressed.
- Disadvantages
  - All disadvantages which apply to Option 1, apply here.
  - The logic of this choice is highly questionable.
  - Difficult, site-specific definitions must be developed which separate things considered to be part of the safeguards system from things considered to influence the performance of the safeguards system. For example, a

CCTV would clearly be a part of the safeguards system. But what about the light bulb in the room which allows the CCTV to function? Upon what grounds would we include or exclude this from the safeguards system? And what about the socket, the wiring, the power source, etc.?

IMPLICATIONS FOR DEFINING CONDITIONS IN BC2

The issue here is the meaning of the requirement in BC2 that licensees must prevent "unauthorized conditions." The meaning of this term depends upon what is included in conditions. If we were to select either the second or third QA options listed above and the definition of containment suggested in the Option Paper of 16 February, nothing which influences safeguards performance would remain to be termed conditions. In this case, our analysis implies that "unauthorized conditions" should be dropped from BC2.

If we select the first QA option, unauthorized conditions include every non-SSNM thing in the facility which could influence safeguards performance. If we select the fourth, we must define conditions in terms of a complex separation of the safeguards system from its immediate environment.