



I 38

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D. C. 20555

February 16, 1977

MEMORANDUM FOR: L. J. Evans, Jr., Chief
Requirements Analysis Branch
Division of Safeguards

FROM: F. J. Arsenault, Assistant Director
for Safeguards
Division of Safeguards, Fuel Cycle
and Environmental Research

SUBJECT: STATUS REPORT--UPGRADE RULE ACTIVITY

The following comments relate to the information copy of your memorandum dated February 10, 1977, subject as above, and its enclosures.

1. With respect to the three options identified in your memorandum, I suggest that the third option be characterized as: "a rule which includes integrated performance requirements and system specifications". This emphasizes that the "integration" is essential to, rather than ancillary to, the third option. It also removes the unnecessary stipulation that the system specifications be "minimum essential". At this stage in the evolution of our regulations, we might well want to go beyond that. I think that the third option is clearly the most desirable.
2. In a memorandum to J. A. Powers dated February 14, 1977, I noted my opinion that your development and expansion of Builder's five capabilities (i.e., your draft performance based rules) were not adequate as regulations but should be used as a basis for a Statement of Consideration. I have held this view although, as that memorandum states, I believe them to be the best existing statement of the intent and purpose of NRC safeguards regulations.

Using performance goals as regulations would require either that we have available an acceptable method of systematically assessing effectiveness, or that we adopt a review and inspection procedure that would be much more analytical, evaluative and flexible than we now have. Effectiveness evaluation techniques that are broadly applicable and validated are many months away. However, two things have happened to suggest that I reconsider my opinion: The first is Ken Chapman's statement that we are moving toward

a review procedure that will be more evaluative, involve more testing and be more effectiveness oriented than compliance oriented. (Of course if we move to performance based rules, the distinction between compliance and effectiveness should tend to disappear.) The second is the detailed list of products and activities included in your memorandum. The list suggests a baseline of guidance which, when combined with the operational changes mentioned above, could well make the evolving rules both viable and effective as regulations.

3. The reason for your distinction (para 2 of your memo) between the "three basic capabilities...developed by A. Poltorak" and the "minimum essential safeguard system specifications... developed by D. Kasun" is not clear. It seems to me that Poltorak has provided performance goals and system requirements for three functions or objectives while Kasun, in an apparently unintegrated and uncoordinated effort, has provided a straw man for a fourth function - reaction and response. I assume the effort was uncoordinated because it overlaps, to a great degree, with Poltorak's three functions.

In the enclosed markup, I have suggested some deletions that would bring Kasun's paper into closer line with the others. If it is desired to retain the details in his Sections B(2), D and E, they could be incorporated into Poltorak's drafts; however, it is my view that they jump a number of steps in the logical unfolding of your performance requirements and should not be included until their need becomes apparent.

Kasun's Section F, Testing, should perhaps be broadened and retained in a form and place applicable to the entire safeguards system.

4. In the enclosed markup, I have suggested some changes that are mainly editorial. However, some points cut into what may have been a carefully deliberated structure and I would like to discuss them with you. In particular, I'd like to discuss the changes suggested for:

- Capability 2, Section A.1 and the similar Capability 3, Section B.1, and

- the integration of Section C with Section B in Capability 3.

Finally, I observe that the use of the word "conditions" in Capability 2 could serve as the basis for the entire "material

L. J. Evans, Jr.

- 3 -

February 16, 1977

control" system as it is defined within the research program. We should discuss whether this is a productive approach or whether some degree of explicit separation is desirable. One question is whether the three capabilities in question are intended to replace 10CFR73 or whether 10CFR70 and 73 will be replaced by a single part that includes more than the three capabilities.

Frank J. Arsenault
Frank J. Arsenault, Assistant Director
for Safeguards
Division of Safeguards, Fuel Cycle
and Environmental Research

Enclosure:
Markup of Drafts

cc w/encl:
K. R. Chapman, NMSS
R. G. Page, NMSS
J. A. Powers, NMSS

Basic Capability 1 Narrative

The safeguard system shall provide the capabilities to ~~prevent~~ ^{protect} ~~against~~ unauthorized personnel entry and prevent introduction of unauthorized material into MAA's and VA's. The licensee must provide access control systems that are able to detect unauthorized attempts to gain access by persons and detect attempts to introduce unauthorized material in sufficient time to permit an effective and acceptable response which prevents unauthorized personnel entry and introduction of unauthorized material.

The following safeguard subsystems are necessary to assure the detection capability. (See Section ___ for necessary aspects of the response capability.)

A. To detect attempts to gain access or introduce material by stealth across MAA and VA boundaries, the following are needed:

1. Access Detection Systems: The licensee shall provide detection systems and procedures that, in a timely manner, will:
 - a.) detect ~~and~~ ^{annunciate} to the reaction and/or response forces any ~~access or penetration~~ ^{to gain access} attempts by persons, or ~~introduce~~ ^{of} material;
 - b.) collect sufficient information for assessment of adversary characteristics and intent;
 - c.) assess the information; and
 - d.) appropriately communicate with reaction and response forces.
2. Barriers: The licensee shall provide barriers that will:
 - a.) channel casual ~~penetration~~ ^{of} persons and material to MAA and VA ~~Entry Controls~~ ^{controlled entry points}; and

b.) delay ~~attempts~~ attempts by persons ~~and to enter~~
introduc~~ion~~ material sufficiently to permit the
detection and response systems to function in an
effective manner.

B. To detect attempts to gain access by deceit into MAA's and
VA's, the following are needed:

1. Access Authorization Controls: The licensee shall provide
authorization controls and procedures for personnel and
material entry that will:

meaning
not clear

- ? {
- a.) establish updated entry requirements;
 - b.) establish accurate authorization schedules based
on routine operational and non-routine/emergency requirements.

2. Entry Controls: The licensee shall provide entry controls
and procedures to:

- a.) verify the identity of persons presenting themselves
for access and/or material presented for introduction;
- b.) assess the verified identity and/or material against
the authorization schedules and entry requirements; and
- c.) appropriately ~~interface~~ interface, with reaction forces.

Basic Capability 2 Narrative

The safeguard system shall provide the capabilities to ~~prevent~~ protect ~~against~~ unauthorized activities and unauthorized conditions within PA's, VA's, and MAA's. The licensee must provide activity and condition control systems that are able to detect unauthorized activities and unauthorized conditions in sufficient time to permit an effective and acceptable response which prevents unauthorized activities and unauthorized conditions to exist or continue.

The following functions are required of the safeguard system to assure the detection capability. (See Section ___ for required functions of the response capability.)

A. To detect unauthorized activities or unauthorized conditions within PA's, VA's, and MAA's, the following are needed:

2. Authorization Controls: The licensee shall ~~provide authorization controls and procedures that will~~ ^{determine and} establish the activities and conditions permitted within each of the ~~areas with~~ ^{defined locations,} unique requirements.

1. Boundaries: The licensee shall define boundaries for the ~~areas~~ ^{locations} that have unique requirements for authorized activities and conditions.

3. Activity and Condition Detection Systems: The licensee shall provide detection systems and procedures that, in a timely manner, will:

a.) surveil monitor and/or inspect each of the defined areas to discover activities and conditions that are not authorized;

b.) collect sufficient information for assessment of the nature of the activity and/or condition;

c.) assess the information; and

d.) appropriately communicate with reaction/response forces.

Basic Capability 3 Narrative

The safeguard system shall provide the capabilities to prevent ~~prevent~~ unauthorized and unconfirmed removal of SNM from MAA's. The licensee must provide removal control systems that are able to detect unauthorized attempts to remove SNM in sufficient time to permit a response, confirm that SNM is being removed in an unauthorized manner, and provide an effective and acceptable response which prevents unauthorized and unconfirmed removal of SNM.

The following safeguard subsystems are necessary to assure the detection and confirmation capabilities. (See Section ___ for necessary aspects of the response capability.)

A. To detect attempts at unauthorized removal of SNM by stealth from MAA's, the following are needed:

1. Removal Detection Systems: The licensee shall provide detection systems and procedures that, in a timely manner, will:
 - a.) detect and annunciate to the reaction and/or response forces any attempts to remove SNM;
 - b.) collect sufficient information for assessment of removal attempt characteristics;
 - c.) assess the information; and
 - d.) appropriately communicate with reaction and response forces.
2. Barriers: The licensee shall provide barriers that will:
 - a.) channel exit attempts to exit controls;
 - b.) delay any attempts to remove SNM sufficiently to permit the detection and response systems to function in an effective manner.

B. To detect attempts at unauthorized removal of SNM by deceit from MAA's, the following are needed:

1. Removal Authorization Controls: The licensee shall ^{determine} ~~provide~~ authorization controls and procedures ~~that will establish accurate properties for~~ authorized removal of SNM by specifying the characteristics of the SNM authorized for removal, the person(s) authorized to remove the SNM, and the removal schedule.
2. Removal Controls: The licensee shall provide removal controls and procedures that will:

- a.) ~~determine~~ ^{verify} the ~~apparent~~ characteristics of the SNM presented for removal;
- b.) verify the identity of the person(s) presenting the SNM for removal;
- c.) ~~verify the removal schedule;~~
- d.) assess the ~~apparent~~ SNM characteristics and the verified identity ~~and removal schedule~~ against the authorized removal properties; and
- e.) appropriately interface with the SNM Confirmation Controls and/or reaction forces.

C. To confirm the identity of SNM presented for authorized removal from MAA's, the following is needed:

1. SNM Confirmation Controls: The licensee shall confirm the authorized removal of SNM by providing controls and procedures that will:
 - a.) verify the apparent characteristics of the SNM presented for removal;

~~b.) assess the confirmed SNM characteristics against the authorized characteristics; and~~

~~c.) appropriately interface with the reaction force.~~

SAFEGUARDS UPGRADE RULE

Minimum Essential Requirements

A. Security Organization

- (1) A security organization including a guard force having the size, armament, equipment, deployment and training capable of clearly defeating the design basis violent assault without outside assistance.
- (2) Liaison with LLEA to insure (i) rapid apprehension (offsite) of attackers (ii) execution of powers of arrest and (iii) assistance against assaults larger than the design basis event.

Accompanying Guides

- Guard force armament, equipment and training
- Guard force size and operation
- Liaison with LLEA

B. Barrier Protection - *Access Denial Systems*

- (1) A system of barriers to delay or deny entrance by personnel and vehicles into the protected area, vital areas and material access areas.
- (2) Penetration resistant vaults for storage and protection of high quality SNM.
- (3) Structures ~~containing alarm, control and~~ defensive positions hardened to prevent penetration by the design basis weapons.
- (4) Area denial systems to protect SNM in process (non-lethal debilitating vapors or liquids)

Accompanying Guides

- Barrier Design
 - PA, VA and MAA (general)
 - Vehicle barriers
 - Vaults
 - Hardening of alarm and control stations
 - Defensive Positions
- Area Denial Systems

C. Communications

- (1) Capability for continuous radio voice communication between the guard force and alarm and control stations and between the facility and LLEA.
- (2) A facility wide tamper-indicating duress alarm system linked to LLEA.

Accompanying Guides

- Duress alarm system

D. Intrusion Alarm System

- (1) An electronic tamper-indicating alarm system for high assurance detection of unauthorized entry (i) into a protected area and (ii) into or within vital areas and material access areas.
- (2) A system for rapid assessment of (i) a perimeter or interior alarm and (ii) the nature and extent of a threat (this includes clear areas, illumination, emergency lighting and CCTV).
- (3) Duplicate independent alarm and control stations

Associated Guides

- Perimeter Intrusion Alarm Systems
- Interior Intrusion Alarm Systems
- Alarm and control stations
- Alarm Assessment

E. Control of Entry and Exit

- (1) A system, including access controls and search of personnel, vehicles, packages and material, to prevent unauthorized entry of personnel, vehicles, weapons and explosives into the protected area, vital areas and material access areas.

- (2) A system, including search of personnel, vehicles, packages and material exiting a material access area, to prevent unauthorized removal of SNM.
- (3) Special containment of high quality, divertible size SNM including isolation of work areas, limited access, surveillance of employees and restrictions on personal articles and clothing (this includes a prohibition against the wearing of metal bearing clothing and the carrying of metal objects thru the material access area exit point).

Accompanying Guides

- Access controls
- Search Techniques and Equipment

F. Testing

- (1) A system, including frequent functional tests, to insure that security equipment sub-systems are operating properly.
- (2) A system to insure that the performance of security organization personnel is adequate.
- (3) A procedure for the integrated testings of the overall facility safeguards system.
- (4) A plan for testing the LLEA response capabilities.

Accompanying Guides

- Alarm System and Communications Testing
- Performance Testing of Security Personnel
- Safeguards System Testing
- Verification of LLEA Response