UNITED STATES
NUCLEAR REGULATORY COMMISSION
ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
WASHINGTON, D. C. 20555

May 19, 1999

The Honorable Shirley Ann Jackson
Chairman
U. S. Nuclear Regulatory Commission
Washington, D.C. 20555-0001

Dear Chairman Jackson:

SUBJECT: THE ROLE OF DEFENSE IN DEPTH IN A RISK-INFORMED REGULATORY SYSTEM

During the 462nd and 461st meetings of the Advisory Committee on Reactor Safeguards, May 5-8 and April 7-10 1999, we discussed issues identified in the Staff Requirements Memorandum dated March 5, 1999, concerning the appropriate relationship and balance between probabilistic risk assessment (PRA) and defense in depth in the context of risk-informed regulation. We previously discussed this matter with the Commission during our meeting on February 3, 1999.

We are attempting to identify pitfalls that may exist along the path the Commission is taking toward risk-informed regulation so they may be addressed in a timely manner. We have communicated previously on the need for plant-specific safety goals that are practical for licensees to evaluate, the need for risk assessments for all modes of plant operation, and the need for research to support further use of risk information in regulatory activities. Several ACRS members, working with an ACRS Senior Fellow, have produced the attached paper in which two views of defense in depth are discussed along with a preliminary proposal regarding its role. Here, we further discuss the role that defense in depth should have in a risk-informed regulatory scheme.

Our motivation for this report has arisen because of instances in which seemingly arbitrary appeals to defense in depth have been used to avoid making changes in regulations or regulatory practices that seemed appropriate in the light of results of quantitative risk analyses. Certainly, we have seen defense in depth used as a basis for delaying changes in the existing regulatory practices:

- there has been reluctance to develop new, risk-informed limits on leakage from steam generator tubes because these are part of the defense-in-depth barriers,

- the development of extensions of the Regulatory Guide 1.174 process to define criteria for risk-informed revisions to 10 CFR 50.59 has been delayed because of defense in depth issues,

- the development of graded quality assurance measures has been overly conservative because of concerns about the imputed importance of quality assurance to defense in depth, and

- the development of regulatory requirements on software-based digital instrumentation and control systems was delayed because of concerns related to defense in depth.

We are concerned that arbitrary appeals to defense in depth could inhibit the effective use of risk information in the regulatory process. At the same time, we are mindful that risk analyses are not perfect. Defense in depth can be an effective means for compensating for any weaknesses in our ability to understand the risks posed by nuclear power plants.

As discussed in the attached paper, the defense-in-depth approach to safety arose in an earlier time when there was less capability to analyze a nuclear power plant as an integrated system. Subsystems were designed such that the necessity and sufficiency of defense in depth could be determined from experience and through exercising engineering judgment. Defense in depth was a design and operational philosophy that called for multiple layers of protection to prevent and mitigate accidents. Its practical implementation was most often associated with control of initiating event frequencies, redundancy and diversity in key safety functions, multiple physical barriers to fission-product release, and emergency response measures. This philosophy has been invoked primarily to compensate for uncertainty in our knowledge of the progression of accidents at nuclear power plants.

Improved capability to analyze nuclear power plants as integrated systems is leading us to reconsider the role of defense in depth. Defense in depth can still provide needed safety assurance in areas not treated or poorly treated by modern analyses or when results of the analyses are quite uncertain. To avoid conflict between the useful elements of defense in depth and the benefits that can be derived from quantitative risk assessment methods, constraints of necessity and sufficiency must be imposed on the application of defense in depth and these must somehow be related to the uncertainties associated with our ability to assess the risk.

We believe that two different perceptions of defense in depth are prominent. In one view (the "structuralist" view as described in the attached paper), defense in depth is considered to be the application of multiple and redundant measures to identify, prevent, or mitigate accidents to such a degree that the design meets the safety objectives. This is the general view taken by the plant designers. The other view (the "rationalist"), sees the proper role of defense in depth in a risk-informed regulatory scheme as compensation for inadequacies, incompleteness, and omissions of risk analyses. We choose here to refer to the inadequacies, incompleteness, and omissions collectively as uncertainties. Defense-in-depth measures are those that are applied to the design or operation of a plant in order to reduce the uncertainties in the determination of the overall regulatory objectives to acceptable levels. Ideally then, there would be an inverse correlation between the uncertainty in the results of risk assessments and the extent to which defense in depth is applied. For those uncertainties that can be directly evaluated, this inverse correlation between defense in depth and the uncertainty should be manifest in a sophisticated PRA uncertainty analysis.

When defense in depth is applied, a justification is needed that is as quantitative as possible of both the necessity and sufficiency of the defense-in-depth measures. Unless defense-in-depth measures are justified in terms of necessity and sufficiency, the full benefits of risk-informed regulation cannot be realized.

The use of quantitative risk-assessment methods and the proper imposition of defense-in-depth measures would be facilitated considerably by the availability of risk-acceptance criteria applicable at a greater level of detail than those we now have. Development of the additional risk-acceptance criteria would have to take into consideration safety objectives embodied in the existing regulations. For example, risk-acceptance criteria are needed to meet the Commission's safety objectives with respect to worker health and environmental contamination and to meet additional public health and safety objectives [e.g., total fatalities, land interdiction]. All of these may not be currently reflected in conventional risk assessments.

We believe that a key missing ingredient needed to place quantitative limits on defense-in-depth measures is acceptance values on the level of uncertainty for each safety objective. Setting such acceptance values is a policy role, very much like setting safety goal values. The uncertainties that are intended to be compensated for by defense in depth include all uncertainties (epistemic and aleatory). Not all of these are directly assessed in a normal PRA uncertainty analysis. Therefore, when acceptance values are placed on uncertainty, these would have to appropriately incorporate consideration of the additional uncertainties not subject to direct quantification by the PRA. These considerations would have to be determined by judgment and expert opinion. As a practical matter, we suggest that the acceptance values be placed on only those epistemic uncertainties quantifiable by the PRA but that these be set sufficiently low to accommodate the unquantified aleatory uncertainties.

When acceptance values have been chosen as policy for the regulatory objectives and their associated uncertainties, it would be possible to develop objective limits on the amount of defense in depth required for those design and operational elements that are subject to evaluation by PRA. To do this, it is necessary to incorporate the effects of the defense-in-depth measures into the PRA uncertainty analysis and the designer or regulator must be able to adjust the defense in depth until the acceptance levels for the regulatory objectives and the acceptance values for the associated uncertainties have both been achieved.

The balance between core damage frequency (CDF) and conditional containment failure probability (CCFP) can serve as an example of this defense-in-depth concept. We have previously recommended that CDF be elevated to a fundamental safety goal. Let us suppose, for example sake, that our acceptance value on this is 10^{-4} per reactor year. If that is the value actually achieved by the design, then a CCFP of about 0.5 has been shown (NUREG-1150) to be generally sufficient to meet the safety goal regulatory objective of individual risk of prompt fatality [which can be adequately represented by an acceptance value of 10^{-5} per reactor year on large, early release frequency (LERF) as noted in Regulatory Guide 1.174]. Does this CCFP provide sufficient defense in depth?

In our view, three acceptance criteria must be satisfied - one each on CDF, LERF, and the epistemic uncertainty associated with LERF. The Safety Goal Policy Statement suggests candidate acceptance values on CDF and LERF. In addition to these, we must establish the acceptance value on the uncertainty associated with LERF. For the particular value of LERF achieved, let's say that the acceptance value has been set by policy to be on the epistemic uncertainty that can be directly developed from the PRA [but which properly reflects the unquantified aleatory uncertainties]. Now suppose our PRA uncertainty analysis tells us that the quantified uncertainty for this design is greater than the acceptance value. Employing our concept, the design with the 0.5 CCFP does not have sufficient defense in depth. The design must, then, include provisions for more defense in depth [e.g., a better containment perhaps] or reduction of the LERF to values for which the achieved uncertainty is acceptable. The acceptance value on uncertainty for any given regulatory objective could be a function of the absolute value achieved for the regulatory objective. That is, as the achieved mean value for LERF gets further below the acceptance value, the acceptable level of uncertainty on its determination can be greater.

We believe this concept of defense in depth can provide a rational way to develop sufficiency limits wherever the defense-in-depth measures can be directly evaluated by PRA. We acknowledge however, that considerable judgment will have to be exercised to set limits on uncertainty, especially uncertainties not quantified by the PRA. Our preceding example suggests one approach to managing these uncertainties.

For those regulatory functions that are not well suited for PRA or where the current capabilities of PRAs are not sufficient, we suggest that the limits on application of defense in depth be placed at levels lower than the top-level safety objectives (see Figure 1 of attached paper). We emphasize that, even under these circumstances, the PRA can still dictate when defense in depth is needed. Let us illustrate how we envision defense in depth to be applied under these circumstances with an example. Fire is one of the initiating events of interest. PRAs quantify the occurrence of fires in nuclear power plants and, among other things, their impact on control and power cables. The plant response to the loss of the relevant systems (due to the loss of these cables) is also analyzed.

The frequency of fires in specific critical locations, that is, locations in which cables of redundant systems may be damaged, is estimated in the PRA using experience-based rates of occurrence of fires, multiplied by subjective estimates of the fraction of fires that are large enough to have the potential to cause damage and the fraction of those fires that occur in the specified critical locations. This is a highly subjective part of the risk assessment (therefore, highly uncertain). It is, therefore, a suitable area to invoke defense in depth and to impose prescriptive requirements regarding the prevention of fires in those critical locations [e.g., strict administrative controls and periodic inspections]. Thus, the relative inadequacy of the PRA model suggests how defense in depth should be applied at levels lower than the top-level safety objectives.

We further realize that the fire risk assessment does not include the damaging effects of the smoke generated by a fire. This is a case of omission of a potentially significant effect. Therefore, we would, again, resort to defense in depth and may demand barriers to limit the spread of smoke and to protect sensitive equipment.

Since the impact on the risk metrics of these lower-level defense-in-depth measures cannot be quantified, nor can the uncertainties, the necessity and sufficiency of the defense-in-depth measures will have to be simply prescribed and that prescription would constitute the acceptance criteria.

We note that our first example dealing with CDF and CCFP addresses the top level of Figure 1 of the attached paper. If one adopts the structuralist viewpoint at that level, as the paper's preliminary proposal suggests, then the tradeoffs of our example between CDF and CCFP will have to be performed under the assumption that at least some level of defense in depth will be required. If, on the other hand, one adopts the rationalist view even at that level, it is conceivable that the LERF objectives could be satisfied without a containment. Our second example dealing with fires exemplified the rationalist view at lower levels, as the preliminary proposal recommends.

We acknowledge that these preliminary thoughts on the role of defense in depth in a risk-informed regulatory system identify a direction but fall short of closing the issue. We recommend that the Commission give further consideration to this matter.

Sincerely,

Dana A. Powers
Chairman

References:

1. U. S. Nuclear Regulatory Commission, Regulatory Guide 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis," July 1998.
2. U. S. Nuclear Regulatory Commission, NUREG-1150, Vols. 1-3, "Severe Accident Risks: An Assessment for Five U. S. Nuclear Power Plants," December 1990.
3. Report dated August 15, 1996, from T. S. Kress, Chairman, ACRS, to Shirley A. Jackson, Chairman, NRC, Subject: Risk-Informed, Performance-Based Regulation and Related Matters.
4. Memorandum dated March 5, 1999, from Annette Vietti-Cook, Secretary of the NRC, to John T. Larkins, Executive Director, ACRS, Subject: Staff Requirements - Meeting with the Advisory Committee on Reactor Safeguards, February 3, 1999.

Attachment:
U. S. Nuclear Regulatory Commission, Advisory Committee on Reactor Safeguards, J. N. Sorensen, G. E. Apostolakis, T. S. Kress, D. A. Powers, "On the Role of Defense in Depth in Risk-Informed Regulation," to be presented at PSA 1999, August 22-25, 1999.

ON THE ROLE OF DEFENSE IN DEPTH IN RISK-INFORMED REGULATION

To be presented at PSA '99
Washington, D.C.
August 22-25, 1999

J. N. Sorensen, Senior Fellow
G. E. Apostolakis, Member
T. S. Kress, Member
D. A. Powers, Member
Advisory Committee on Reactor Safeguards
U. S. Nuclear Regulatory Commission
Washington, D.C. 20555-0001

ABSTRACT

The nascent implementation of risk informed regulation in the United States suggests a need for reexamination of the Nuclear Regulatory Commission's (NRC) defense in depth philosophy and its impact on the design, operation, and regulation of nuclear power plants. This reexamination is motivated by two opposing concerns: (1) that the benefits of risk informed regulation might be diminished by arbitrary appeals to defense in depth, and (2) that the implementation of risk informed regulation could undermine the defense in depth philosophy. From either perspective, two questions are suggested: (1) How is defense in depth defined? (2) How should the implementation of risk informed regulation alter our view of defense in depth? A preliminary proposal for the role of defense in depth in a risk-informed regulatory system is presented.

HISTORICAL DEVELOPMENT

Defense in depth is a nuclear industry safety strategy that began to develop in the 1950s. A review of the history of the term indicates that there is no official or preferred definition. Where the term is used, if a definition is needed, one is created consistent with the intended use of the term. Such definitions are often made by example.

In a 1967 statement[1] submitted to the Joint Committee on Atomic Energy by Clifford Beck, then Deputy Director of Regulation for the Atomic Energy Commission, three basic lines of defense for nuclear power reactor facilities were described. The first line was the prevention of accident initiators through superior quality of design, construction and operation. The second line was engineered safety systems designed to prevent mishaps from escalating into major accidents. The third line was consequence-limiting safety systems designed to confine or minimize

the escape of fission products to the environment.

A 1969 paper[2] by an internal study group of the Atomic Energy Commission identified the issue of balance among accident prevention, protection, and mitigation, with the conclusion that the greatest emphasis should be put on prevention, the first line of defense.

A 1994 NRC document[3] identifies the elements of the defense in depth safety strategy as accident prevention, safety systems, containment, accident management, and siting and emergency plans. Other interpretations of defense in depth can be found in INSAG-3[4] and INSAG-10[5]

The historical record indicates an evolution of the term from a narrow application to the multiple barrier concept to an expansive application as an overall safety strategy. The term has increased in scope and gained stature over time. The history also indicates that defense in depth is considered to be a concept, an approach, a principle or a philosophy, as opposed to being a regulatory requirement per se.

Currently the term is commonly used in two different senses. The first is to denote the philosophy of high level lines of defense, such as prevent accident initiators from occurring, terminate accident sequences quickly, and mitigate accidents that are not successfully terminated. The second is to denote the multiple physical barrier approach, most often exemplified by the fuel cladding, primary system, and containment.

One of the essential properties of defense in depth is the concept of successive barriers or levels. This concept applies equally well to multiple physical barriers and to high level lines of defense. A closely related attribute would be requiring a reasonable balance among prevention, protection and mitigation.

EMERGING REGULATORY PRACTICE

The most recent NRC policy statement that deals with defense in depth is the Probabilistic Risk Assessment (PRA) Policy statement[6] published in 1995, which states, in part:

"The use of PRA technology should be increased in all regulatory matters to the extent supported by the state-of-the-art in PRA methods and data and in a manner that complements the NRC's deterministic approach and supports the NRC's traditional defense-in-depth philosophy."

The policy statement, thus, places PRA in a subsidiary role to defense in depth.

In 1998, the NRC published Regulatory Guide 1.174.[7] This guide establishes an approach to risk-informed decision making, acceptable to the NRC staff, which includes the provision that proposed changes to the current licensing basis must be consistent with the defense in depth philosophy. The RG 1.174

discussion states that, "The defense in depth philosophy . . . has been and continues to be an effective way to account for uncertainties in equipment and human performance." The discussion goes on to say that PRA can be used to help determine the appropriate extent of defense in depth, which, by example, is equated to balance among core damage prevention, containment failure prevention and consequence mitigation. The regulatory guide thus addresses the concern of preventing risk-informed regulation from undermining defense in depth. Defense in depth is primary, with PRA available to measure how well it has been achieved.

STRUCTURALIST MODEL

We have identified two different schools of thought (models) on the scope and nature of defense in depth. These models came to be labeled "structuralist" and "rationalist."

The structuralist model asserts that defense in depth is embodied in the structure of the regulations and in the design of the facilities built to comply with those regulations. The requirements for defense in depth are derived by repeated application of the question, "What if this barrier or safety feature fails?" The results of that process are documented in the regulations themselves, specifically in Title 10, Code of Federal Regulations. In this model, the necessary and sufficient conditions are those that can be derived from Title 10. It is also a characteristic of this model that balance must be preserved among the high-level lines of defense, e.g., preventing accident initiators, terminating accident sequences quickly, and mitigating accidents that are not successfully terminated. One result is that certain provisions for safety, for example reactor containment and emergency planning, must be made regardless of our assessment of the probability that they may be required. Accident prevention alone is not relied upon to achieve an adequate level of protection.

There does not appear to be any question that the implementation of defense in depth up to the present time reflects the structuralist model. While this philosophy has served the industry well from the safety perspective, it is now realized that, in some instances, it has led to excessive regulatory burden. Furthermore, the lack of an integrated view of the reactor systems has resulted in some significant accident sequences not being identified until PRA was developed, e.g., the interfacing-systems LOCA sequence.

The next issue, then, becomes how should the insights from PRA be integrated into this structure to reduce unnecessary burden and make it more rational? In the structuralist model, defense in depth is primary, with PRA available to measure how well it has been achieved.

THE RATIONALIST MODEL

The rationalist model asserts that defense in depth is the aggregate of provisions made to compensate for uncertainty and incompleteness in our knowledge of accident initiation and progression. This model is made practical by the development of the ability to quantify risk and estimate uncertainty using probabilistic risk assessment techniques. The process envisioned by the rationalist is: (1) establish quantitative acceptance criteria, such as the quantitative health objectives, core damage frequency and large early release frequency, (2) analyze the system using PRA methods to establish that the acceptance criteria are met, and (3) evaluate the uncertainties in the analysis, especially those due to model incompleteness, and determine what steps should be taken to compensate for those uncertainties. In this model, the purpose of defense in depth is to increase the degree of confidence in the results of the PRA or other analyses supporting the conclusion that adequate safety has been achieved.

The underlying philosophy here is that the probability of accidents must be acceptably low. Provisions made to achieve sufficiently low accident probabilities are defense in depth. It should be noted that defense in depth may be manifested in safety goals and acceptance criteria which are input to the design process. In choosing goals for core damage frequency and conditional containment failure probability, for example, a judgement is made on the balance between prevention and mitigation.

What distinguishes the rationalist model from the structural model is the degree to which it depends on establishing quantitative acceptance criteria, and then carrying formal analyses, including analysis of uncertainties, as far as the analytical methodology permits. The exercise of engineering judgement, to determine the kind and extent of defense in depth measures, occurs after the capabilities of the analyses have been exhausted.

A PRELIMINARY PROPOSAL

The structuralist and rationalist models are not generally in conflict. Both can be construed as a means of dealing with uncertainty. Neither incorporates any reliable means of determining when the degree of defense in depth achieved is sufficient. In the final analysis, they both depend on knowledgeable people discussing the risks and uncertainties and ultimately agreeing on the provisions that must be made in the name of defense in depth. The fundamental difference is that the structural model accepts defense in depth as the fundamental value, while the rationalist model would place defense in depth in a subsidiary role.

The remaining question is which model provides the better basis for moving forward with risk- informed regulation. How can capricious imposition of

defense-in-depth be prevented from undermining the focus that can be provided by risk- informed methods of regulation? PRA methods have identified gaps in the regulations and in the safety profiles of individual plants. They have also identified regulations and plant systems that do not make a significant contribution to safety. Typically, however, regulatory reactions to findings that regulations or plant systems are superfluous to safety have been less aggressive than reactions to apparent safety deficiencies.

Two options can be identified:

(1) Recommend defense in depth as a supplement to risk analysis (the rationalist view)

(2) Recommend a high-level structural view and a low-level rationalist view.

Option (1) requires a significant change in the regulatory structure. The place of defense in depth in the regulatory hierarchy would have to change. The PRA policy statement could no longer relegate PRA to a position of supporting defense in depth. Defense in depth would become an element of the overall safety analysis.

Option (2) is to a large degree compatible with the current regulatory structure. The structuralist model of defense in depth would be retained as the high-level safety philosophy, but the rationalist model would be used at lower levels in the safety hierarchy. An example is shown in Figure 1.

The PRA uncertainties increase as we move from the initiating events to risk (from left to right). The structuralist view dictates that intermediate goals be set, such as core damage frequency (CDF), large early release frequency (LERF) or conditional containment failure probability (CCFP),or frequency-consequence (F-C) curves. This would satisfy the requirement of balance between prevention and mitigation. We note that the actual numerical value chosen for core damage frequency can express a preference for prevention, and such a preference is unrelated to defense in depth. One could proceed and set goals at the "cornerstone" level, i.e., one level below. This could include goals on initiating- event frequencies, safety-function or safety-system unavailabilities, and so on. How far down one would go would be a policy issue. The structuralist view would not be applied at lower levels.

The rationalist model would be applied at levels lower than the cornerstones of Figure 1. Defense in depth would be used only to address uncertainties in PRA at the lower levels, thus becoming an element of the overall safety analysis. For events or processes that are not modeled in PRA, defense in depth would play its traditional role. Such is the case with the impact of smoke from fires on plant safety. Current fire risk assessments do not account for the effects of smoke, therefore, prescriptive defense-in-depth based

measures would be taken to limit this impact.

We view Option (2) as a pragmatic approach to reconciling defense in depth with risk-informed regulation. There can be little doubt, however, that the rationalist model, Option (1), will ultimately provide the strongest theoretical foundation for risk-informed regulation. When more experience has been gained with the application of PRA in the design and regulation of nuclear power plants, when PRA models can adequately treat most of the phenomena of interest, the role of defense in depth can and should be changed to one of supporting the risk analyses. This transition will need to be supported by the development of subsidiary principles from which necessary and sufficient conditions could be derived.

Note

The views expressed in this paper are the authors' and do not necessarily represent the views of the Advisory Committee on Reactor Safeguards

REFERENCES

1. C. Beck, "Basic Goals of Regulatory Review: Major Considerations Affecting Reactor Licensing," Statement submitted to the Joint Committee on Atomic Energy, Congress of the United States, Hearings on Licensing and Regulation of Nuclear Reactors, April 4 5,6,20, and May 3, 1967.

2. Internal Study Group, "Report to the Atomic Energy Commission on the Reactor Licensing Program," submitted to the Joint Committee on Atomic Energy, Congress of the United States, Hearings on AEC Licensing Procedure and Related Legislation, June 1969.

3. F. E. Haskin, and A. L. Camp,, "Perspectives on Reactor Safety," NUREG/CR-6042, Nuclear Regulatory Commission, Washington, DC, March 1994.

4. International Nuclear Safety Advisory Group, "Basic Safety Principles for Nuclear Power Plants," Safety Series No. 75-INSAG-3, International Atomic Energy Agency, Vienna, Austria, 1988

5. International Nuclear Safety Advisory Group, "Defense in Depth in Nuclear Safety," INSAG-10, International Atomic Energy Agency, Vienna, Austria, 1996

6. U. S. Nuclear Regulatory Commission, "Use of Probabilistic Risk Assessment in Nuclear Regulatory Activities; Final Policy Statement," Federal Register, 60 FR 42622

7. U. S. Nuclear Regulatory Commission, "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Current Licensing Basis," Regulatory Guide 1.174, June 1998

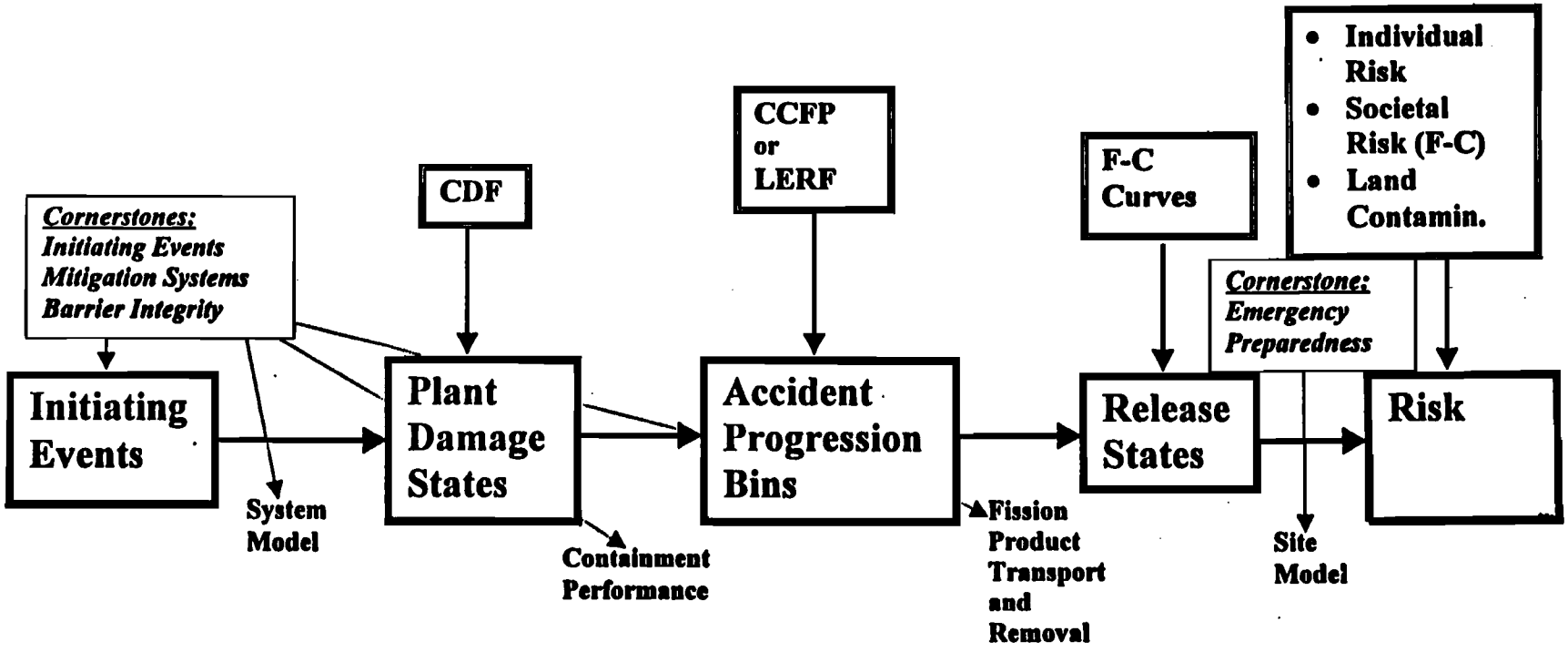

Figure 1. Possible implementation of the structural model at a high level.