

RECEIVED

'99 DEC 23 AIO:26

PUBLIC DOCUMENT

---

---

# **A Structured Approach for Review of Digital Plant Protection System Requirements Specifications**

---

---

**Volume 1: Overview**

**August 31, 1999**

**Robert W. Brill, NRC  
Ray Berg, SNL  
Gary Johnson, LLNL**

### Disclaimer

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor the University of California, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the University of California and shall not be used for advertising or product endorsement purposes.

This work was supported by the United States Nuclear Regulatory Commission under a Memorandum of Understanding with the United States Department of Energy, and performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract W-7405-Eng-48.

# **A STRUCTURED APPROACH FOR REVIEW OF DIGITAL PLANT PROTECTION SYSTEM REQUIREMENTS SPECIFICATIONS VOLUME 1: OVERVIEW**

## **BACKGROUND**

Instrumentation and control (I&C) systems provide monitoring, control, and protection functions in nuclear power plants (NPPs). Most existing nuclear power plant I&C systems were designed using analog devices. However, parts for these analog systems are becoming unavailable due to obsolescence and their maintenance costs are increasing, so nuclear utilities are upgrading to digital systems. Digital systems offer several advantages over existing analog systems. For example, digital systems are essentially free of the drifts associated with analog systems, have higher data handling and storage capabilities, and provide improved system performance in terms of accuracy and computational capabilities. As would be expected, new technologies bring new challenges that must be considered such as sampling rate considerations, cycle times, discreteness of monitored parameters, greater susceptibility to environmental effects, and computer software quality.

In the design and review of any complex safety-related system, it is vitally important to specify, clearly and accurately, the fundamental functions that the system is supposed to accomplish. These high-level requirements must be traceable from the system level, through subsystem layers, to the individual component that performs the function. If this is not done, serious undetected errors can creep into a digital system design, and the system may fail at a crucial moment. Studies indicate that the majority of all software errors are caused by incorrect or incomplete requirements.

## **PROBLEM**

Systems engineering methods have not been developed to ensure that NPP protection system and software requirements are complete, consistent, and correct. Frequently, the cause of software requirements errors can be traced to incomplete or incorrect system requirements.

## **NRC NEED**

Section 7 of the Standard Review Plan (SRP) for nuclear power plants states the need to review requirements at various levels. However, acceptance criteria for these reviews are very high-level, requiring mainly completeness and consistency with little specific guidance on how to determine if these characteristics are achieved. Yet, in the review of such systems NRC must address several new review considerations such as sampling effects, cycle times, discreteness of monitored parameters, and computer software quality.

## **OVERVIEW OF PROJECT**

This project was initiated in response to work done by Leo Beltracchi of the Nuclear Regulatory Commission to apply a means-ends hierarchical approach to the specification of nuclear power plant I&C safety systems (Beltracchi 1996), which built upon the work of Rasmussen (1987). Rasmussen proposed a method of developing system requirements by beginning with an abstract definition of system purpose, and then, through a series of steps, decomposing the abstract purpose into progressively more concrete and explicit terms until a complete and unambiguous specification is obtained. This approach is intended

to ensure that requirements specifications are complete, and provides visible traceability between detailed specifications and high-level functional requirements.

Sandia National Laboratory (SNL) developed an initial version of the Structured Approach incorporating the ideas of Beltracchi and Rasmussen (Staple 1997). In parallel with this effort, Lawrence Livermore National Laboratory (LLNL) examined existing system engineering approaches and standards to identify issues to be considered in the review of the Sandia approach (Scott 1997). After the initial SNL and LLNL efforts were completed, the NRC refocused the effort from developing a specification methodology to developing a review method that could be used by NRC staff. This spurred the development of a more practically oriented, less academic description of the model. SNL and LLNL collaborated in refocusing and recasting the Structured Approach to this effect (Berg 1998). LLNL, in collaboration with the University of California at Berkeley (UCB), performed a trial application of this method to the Advanced Boiling Water Reactor (ABWR) protection systems (documented in Volume 3 of this report). This trial application demonstrated that the Structured Approach supported a very broad review of protection system requirements and established traceability between requirements and fundamental safety objectives. The trial application identified a number of changes to the approach that were necessary to make it more complete and usable, and the Structured Approach was then modified accordingly. Volume 2 of this report describes the modified method.

An important finding of the trial application is that applying the Structured Approach review specifications is very labor-intensive. Reviewing the ABWR requirements specifications involved approximately 20 staff-weeks of effort, not including time required to develop data collection tools, the framework topic dictionary, or reports. The extensive effort was required, to a large extent, because safety analyses and requirements specifications are not well organized to support the specifications review envisioned by the Structured Approach. These documents are well organized to accomplish their primary purpose of supporting the plant safety case and for supporting the design and procurement of equipment. It would be inappropriate to reorganize these documents to better support requirements reviews, to the detriment of their primary purpose. Therefore, review methodologies need to account for the difficulty of finding relevant information in plant documentation.

Using requirements management tools to organize requirements and traceability analyses, so that different users of the requirements can view the requirements from different perspectives, might allow the review process to be simplified while preserving the organization that is needed for the analysts and developers. However, investigating tools that might allow this capability was beyond the scope of this project.

## **GENERAL APPROACH**

In performing a "thread" audit, the reviewer must be able to trace a system requirement, from its genesis in the system requirements, through the allocation of functions, through the functional specifications, the specific module specifications, into the architectural design, coding and testing. The Structured Approach provides a systems engineering technique for extracting the requirements from the system level through the module requirements level. In using the Structured Approach the reviewer first addresses the system-level requirements, then again uses it at the module level. (The process is identical at all stages.)

The Structured Approach is based on the concept that the developer will have (1) begun with determining the hazards to a NPP, (2) designed plant protection systems for mitigation and defense against those hazards, (3) identified the hazards to the protection systems, and finally (4) designed mitigation and defense against the hazards to the protection system.

In using the Structured Approach, the reviewer derives the requirements expected from NPP safety and system analyses by completing two sets of linked tables. These tables are generated by following a nine-step process. Each step uses either specific information from the existing NPP safety analyses and the previous steps or is derived from the previous steps. The information at each step, or level, is collected into one or more tables.

One set of tables defines the expected functional requirements, and compares them to system design bases and component requirements specifications. Functional requirements are predominately derived from assumptions of, or results from, the accident analyses contained in the Final Safety Analysis Reports (FSAR) Chapter 17 and protection system architecture described in FSAR Chapter 7 (including in both cases referenced materials such as topical reports).

The second set of tables defines the expected integrity requirements, and compares them to system design bases and component requirements specifications. There are several different kinds of integrity requirements:

- Requirements to defend against protection system component failures — described in FSAR Chapter 7
- Requirements to cope with normal and abnormal ambient environments — described in FSAR Chapters 3, 9, and 12
- Requirements to cope with accident ambient environments — described in FSAR Chapters 3 and 12
- Requirements to cope with the effects of natural phenomena hazards — described in FSAR Chapter 3
- Requirements to cope with process environment hazards — described in FSAR Chapters 4, 5, and 10.
- Requirements to cope with the normal and abnormal electromagnetic environment — described in FSAR Chapter 7
- Requirements to cope with variations in power supply conditions — described in FSAR Chapter 8.

## **DETAILED APPROACH**

The Structured Approach provides a technique for forward traceability from plant hazards to functional and integrity requirements for NPP protection systems. It makes use of the fact that plant design assumptions and analyses, primarily those summarized in Chapter 15 of the FSAR, identify the high-level functional requirements (both the functions to be performed and the performance required of those functions) necessary to (1) ensure the integrity of the reactor coolant pressure boundary, (2) ensure the capability to shut down the reactor and maintain it in a safe shutdown condition, and (3) prevent or mitigate the consequences of accidents.

Also, most of the information required to identify the functional and integrity requirements already exists as part of licensees' licensing basis documents (LBDs). These safety analyses exist as part of the licensing basis for existing plants, and are produced as part of the licensing process for new plants. Therefore, the Structured Approach is useful for reviewing both digital I&C retrofits to existing plants and digital I&C designs for new plants.

Figures 1a and 1b show the nine steps in the Structured Approach, together with the ties to the Standard Review Plan. Figure 1a shows the first five steps, which extract the functional requirements. Although the steps are described sequentially, there may be some need to conduct parts in parallel. For example, it may be necessary to study the top level protection system architecture (step 3) to some extent in order to understand the relationship of accident analyses to protection system functions (steps 1 and 2). Figure 1b shows the last four steps, which extract the integrity requirements. Figure 2 shows the application of the Structured Approach from the user perspective.

## Functional Requirements (Steps 1 through 5)

- Step 1 The Structured Approach begins with a review of accident analyses to identify protection system functional requirements. This review extracts information about the protection system functions and performance assumed in the accident analysis, and the dynamic characteristics of plant parameters that establish requirements for the protection system's functions. For example, the CE System 80+ accident analysis assumes that in the event of loss of condenser vacuum, emergency feedwater actuation occurs within 600 msec of steam generator water level dropping below 19.9 ft. The analysis includes assumptions (e.g., initiation delay time) about the performance. Information is extracted for each potential initiating event (PIE) under consideration, and the result is a set of level-1 tables describing the limiting characteristics of each PIE. One table will be generated for each PIE under review.
- Step 2 The protection system requirements are identified by deriving them from the analyses of the PIEs described above. By analyzing the information collected in the level-1 tables, reviewers can extract the limiting cases that describe the protection system functional requirements for the specific protection system function. For example, emergency feedwater initiation on low steam generator water level is assumed for both loss of condenser vacuum and loss of offsite power. The limiting rate of change of steam generator water level change that the I&C system must cope with is established by the loss of vacuum event at 3 ft/sec. The result is a set of level-2 tables describing the system's top-level functional requirements.
- Step 3 The top-level protection system architecture is reviewed to identify how the required functions, extracted from the above tables, are allocated to the protection system subsystems, e.g., reactor trip system and engineered safety feature actuation system. The subsystem assignment information is then added to the level-2 table that describes the functional requirements for the protection system function under review, to produce a level-3 table. For example, in the CE System 80+ the emergency feedwater initiation is a function of an integrated engineered safety features actuation system, and the requirements extracted by studying the loss of offsite power and loss of condenser vacuum events apply to this system. One level-3 table is generated for each protection system function under consideration, so there is a 1:1 correspondence with the level-2 tables.
- Step 4 The functional requirements that were identified in steps 1 and 2, knowledge about the protection system design, and knowledge of interface requirements from the mechanical engineered safety features systems, are used to develop functional requirements for any specific component that is being considered for review. For example, the bistable trip device associated with the emergency feedwater actuation on low steam generator water level must have a response time of less than 600 msec. The information in the level-3 table of functional requirements is used to create a new, level-4 table describing the functional requirements for particular protection system component(s) selected for review. (These may be hardware, or software components, or humans carrying out procedures.) Note that the functional requirements

for any component are strongly dependent upon the component's role in the system architecture. In the case of the bistable trip device, its response time must not only be less than 600 msec, but it must be less than 600 msec minus all of the other delays in the trip string. As part of this step, the reviewer uses the Requirements Topics<sup>1</sup> (provided in Volume 2) to convert each high-level requirement identified by previous steps into specific requirements for the component under consideration. (For example, the high-level assumption of an overall trip time delay for a function will map to sample rate and execution time requirements for individual hardware and software elements of the protection system.) In all cases the functional requirements identified by the analysis in steps 1 through 3 must be appropriately reflected in lower-level requirements.

The list of expected requirements collected in the level-4 tables is evaluated against the actual specification for the component(s) under review (step 5a) to create a level-5a set of tables. For example, the specification of the bistable trip device must require a response time of much less than 600 msec. (This step contains the actual component functional requirements reviews, after all of the pertinent information has been generated in steps 1 through 4 above.)

Note that if an expected functional requirement listed in the level-4 table is not addressed by the component specification, this is an indication that the specification is incomplete. Conversely, if all expected requirements are addressed by the specification, the review provides assurance that the functional requirements in the component specification are reasonably complete, although the process cannot guarantee completeness.

- Step 5b As in step 5a, the design basis requirements from the FSAR and the function assignments from the level-3 tables are compared to the functional requirements derived from the safety analyses. For example, the design basis for emergency feedwater actuation must specify that the function shall be initiated on low steam generator water level with a delay time of less than 600 msec. (This step contains the balance of the actual component functional requirements reviews, after all of the pertinent information has been generated in steps 1 through 4 above.)

### **Integrity Requirements (Steps 6 through 9)**

- Step 6 The hazards to protection system integrity are determined by examining safety and system analyses. Information from this analysis is recorded in a set of level-6 tables that identify integrity hazards posed by hardware (e.g., random failure of a bistable device such that it will not trip); software (e.g., incorrect implementation of a trip algorithm); normal, abnormal, and accident environments (e.g., normal, abnormal, and accident temperature); process environments (e.g., the corrosive properties of the sensed fluid); and power supplies (e.g., voltage transients).
- Step 7 The top-level protection system architecture and FSAR are reviewed to identify how the integrity hazard characteristics, extracted from the level-6 tables, are allocated to the protection system design features (e.g., random failures may be addressed by a combination of redundancy, isolation, and surveillance testing). This information is then added to the level-6 tables to produce level-7 tables. There is a 1:1 correspondence between this information and the level-6 tables. Additional design features that were assumed in the system analysis of step 6 must also be identified and added to the tables.

---

<sup>1</sup> A Requirements Topic is the *description* of a specific requirement. For example, a sensor is required to measure a specific range of inputs. The Requirements Topic states that the sensor specification must include a requirement describing the range of inputs to be measured.

- Step 8 The hazards to protection system integrity that were codified in the level-7 tables are used to develop level-8 tables that describe the integrity hazards that must be addressed by the particular protection system components selected for review. For example, a bistable trip device must have provisions to allow the surveillance testing to deal with the possibility that it may randomly fail. The reviewer's understanding of the system architecture and the component's role in that architecture is used to identify the hazards that must be addressed in the requirements for the component under consideration. The reviewer then uses the Catalog of Requirements Topics to identify specific Requirements Topics that address the identified integrity hazards. All integrity requirements for a given design element must be appropriately reflected in lower-level requirements.
- Step 9a The list of expected requirements that were collected in the level-8 tables is evaluated against the actual specification for the component(s) under review. For example, the specification for a bistable trip device must describe the automatic surveillance test functions to be performed, and must specify the types of connections and controls to be provided to enable manual surveillance tests. That information is collected into a level-9a set of tables. If an expected integrity requirement listed in a level-8 table is not addressed by the component specification, this is an indication that the specification is incomplete. Conversely, if all expected requirements are addressed by the specification, the review provides assurance that the integrity requirements in the component specification are reasonably complete, although the process cannot guarantee completeness.
- Step 9b The design basis requirements from the FSAR and the characteristics of integrity hazards from the level-6 tables are similarly compared to the integrity requirements derived from the safety analyses, to create a series of level-9b tables. For example, the design basis should contain requirements for the types and frequency of surveillance testing to be performed to address the possibility of random failure of bistable trip devices.

## **TRIAL APPLICATION OF THE STRUCTURED APPROACH**

The ABWR Standard Safety Analysis Report (SSAR) formed the basis for a review of the protection system specifications for the Kashiwazaki-Kariwa Nuclear Power Generating Station, Units 5 and 6. This trial application succeeded in applying the Structured Approach to the review of an actual set of protection system specifications. It demonstrated the feasibility of the Structured Approach and succeeded in identifying where further refinement of the approach is needed. Most of these refinements have been incorporated into the Structured Approach, as described in Volume 2 of this report. Some of the needed refinements are beyond the defined work scope for this project and, therefore, must be left for future development.

### **Strengths of the Structured Approach**

The Structured Approach led to a fairly thorough review of the design issues for the plant protection systems, and highlighted areas for further investigation that may not have been identified in a more casual review. The analysis maintained traceability of specification requirements to the plant safety analyses and protection system failure analyses. A major benefit of the Structured Approach is that it forces the reviewer to develop a complete understanding of the design and the basis for the design.

Had the trial application been an actual review, the application of the Structured Approach would have resulted in requests for additional information in the following areas:

- Design bases for protection system functions that are not explicitly credited in the accident analyses of the safety analysis report.
- Design bases for ancillary functions of the protection system such as interlocks, permissives, and control functions.
- Response time requirements.
- Communications interface requirements.
- Environmental requirements.
- Electromagnetic interference environments and protection methods.
- Setpoint analysis assumptions.

Many of the questions raised relate to information needed about plant safety characteristics. Generally, where information was available on both the fundamental safety requirements and specification requirements, the specification requirements were found to be consistent with safety analyses assumptions and findings. In cases where such consistency was not found, a number of possible rationales for the inconsistencies are possible and would be investigated in the course of an actual review.

The questions raised by the trial application of the Structured Approach should not be taken as a reflection on the ABWR SSAR, ABWR design, or the NRC review. A typical requirements review would have a narrower focus than this trial; therefore, additional questions were expected to be found by this more extensive review. Establishing confidence in a plant design does not require that the NRC staff identify and resolve every possible open item. Rather, the intent is to perform a review that is broad enough to provide confidence in the applicant's design processes and to identify issues of high safety significance.

### **Weaknesses of the Structured Approach**

The trial application succeeded in testing the Structured Approach, indicating both areas of strength and potential pitfalls or aspects that need to be redesigned. The Structured Approach collects insufficient data regarding exactly what functions must be performed. It identifies the functions generically (e.g., initiate reactor core isolation cooling) but does not specify the specific functions required of protection system functions (e.g., data transformations, or output of command sequences). This is an important lack of completeness as it provides no basis to review the specific algorithms or command logic that must be implemented by the protection system. To develop these requirements, the necessary functions of the mechanical engineered safety feature systems must be defined along with their performance requirements and integrity strategies. Incorporating these elements into the Structured Approach was beyond the scope of this project. From a review standpoint, it may be more reasonable to perform a confirmatory review that the required protection system actions will result in proper alignment of the associated engineered safety feature systems.

Using the applicant's failure analysis to identify hazards from protection system failures *did* identify hazards that pose significant threats to the baseline design of the protection system, but did *not* identify hazards that were already addressed by the baseline design — for example, hazards addressed by compliance with accepted practices, such as those defined by IEEE Std. 603. In this regard, the Structured Approach identified a very incomplete set of integrity requirements for the protection system.

The Structured Approach does not consider design choices that must be documented in order to ensure proper functional interfaces between protection system components and subsystems. These design choices

generally do not derive directly from safety analysis assumptions or results; they are determined by the designer. The Structured Approach should confirm that the choices made are consistent with the fundamental safety requirements and are consistently implemented across all system components.

The Structured Approach was difficult to implement because it requires familiarity with an extensive set of input documentation, and the organization of existing safety analysis documentation poorly supports the Structured Approach. The information needed to perform the review is scattered throughout the SSAR and many specification documents. Implementing the review for one specific function would require familiarity with tens of documents and the examination of many tens more to locate the required set. Consequently, the Structured Approach as defined is probably too burdensome to be a practical review tool for the NRC.

Knowledge gained from the trial application suggested the means to develop a practical requirements review tool — a set of review templates using concepts from the Structured Approach that could be used by NRC staff in actual reviews. The templates would identify the critical requirement topics that the reviewer expects specifications to cover. The Structured Approach process for extracting protection system functional requirements based upon accident analysis assumptions and results would be used in a simplified form appropriate for performing trace audits of functional requirements. Integrity requirement checklists could be developed based upon the guidance of IEEE Std. 603, IEEE Std. 7-4.3.2, and their supporting standards. Generic checklists could be developed for typical protection system architectures and design elements. Such checklists would address most systems because using the IEEE standards is essentially mandated by 10 CFR 50.55a(h), and considerable commonality exists between the system architectures from the various vendors. The templates would assist reviewers in confirming that system and component specifications are consistent with the requirements of 10 CFR 50.55a(h) (IEEE Std. 603 as supplemented by IEEE Std. 7-4.3.2). These templates would be used to conduct reviews in accordance with SRP Section 7.1-C.

## **NRR USE OF THE STRUCTURED APPROACH IN A REVIEW**

Figure 2 gives an overview of the use of the Structured Approach for reviewing protection systems' design bases and protection system components specifications. The Structured Approach may be applied to review any element of a protection system design, from a large subsystem down to an individual part or software routine. The following discussion gives a brief description of how the Structured Approach is used in performing the review tasks illustrated in Figure 2, and relates these review tasks to the Figure 1 analytical steps.

1. One or more protection system functions is selected for examination in the review.
2. The safety system requirements applicable to the function(s) under consideration are developed by examining the Safety Analysis Report and supporting documents. Both functional requirements (analytical steps 1 through 3 as shown in Figure 1) and integrity requirements (analytical steps 6 through 7) are examined to identify the safety requirements.
3. After safety system requirements are collected for the selected functions the design basis requirements are reviewed. This is performed by comparing the functional and integrity requirements (extracted from the safety analyses) with the design basis requirements presented by the applicant or licensee (analytical steps 5b and 9b). If the design basis requirements do not encompass all of the requirements extracted from the safety analysis review, then the design basis is inconsistent with the plant safety analyses. Such a finding should call into question the adequacy of the applicant or licensee's engineering process as well as the adequacy of the design basis itself or the adequacy of the

design basis documentation.

4. The system components that will be included in the scope of the review are selected. The requirements are then derived for the selected protection system-specific component(s).<sup>2</sup>
5. Components that have been defined by the licensee or applicant are typically selected for review, because design documents and requirements specifications will usually best reflect the licensee or applicant's system partitioning. Once a component to be reviewed is selected, the system requirements applicable to that component are identified by considering the component's role in the system and identifying the safety system requirements that the component has a role in fulfilling.<sup>3</sup>
6. Component safety requirements are derived by examining safety system requirements applicable to the component and identifying the Specification Topics<sup>4</sup> that must be defined to address these system requirements. Determining component safety requirements includes both functional requirements (analytical step 4) and integrity requirements (analytical step 8) using the Requirements Topic Library.<sup>5</sup>
7. After component safety requirements are collected for the selected functions, component specifications are reviewed. The component functional and integrity requirements developed using the taxonomy of Requirements Topics (analytical step 5a) are compared with the component specifications developed by the licensee or applicant (analytical step 9a) to perform the review.

The Structured Approach thus provides a systems engineering approach to performing a top-down traceability review from systems requirements through software and hardware requirements specifications. The reviewer could select a particular function to examine, trace the systems requirements into a particular software requirements specification, select the module for review, and examine its requirements specification. For example, assume a system requirement exists for a reactor protection system. Then assume that the allocation of functions places part of the logic into a software requirement. This software requirement usually results in a requirement for a bistable processor module. The bistable module then decomposes into a standard set of sub-modules, as shown in Figure 3. In the figure, note the Engineering Units Conversion sub-module. Using the Structured Approach, one of the tables for this module would be example table B4 in Volume 2.

The specifications must encompass all of the requirements extracted from the safety analysis review. If they do not, the specification is inconsistent with the plant safety analyses. Such a finding will require correction to the specifications and call into question the adequacy of the applicant or licensee's requirements engineering process.<sup>6</sup>

---

<sup>2</sup> The component selected may be a hardware component, a software component, a human activity controlled by procedure, or a functional unit that integrates more than one of these components.

<sup>3</sup> Some system-level requirements, such as redundancy, are almost completely addressed at the system-architecture level, and redundancy requirements impose no specific technical requirements on a low-level component. Other system-level requirements, such as diversity, will impose requirements at the component level. In this case, the restrictions on the implementation methods and technologies needed to ensure diversity must be specified.

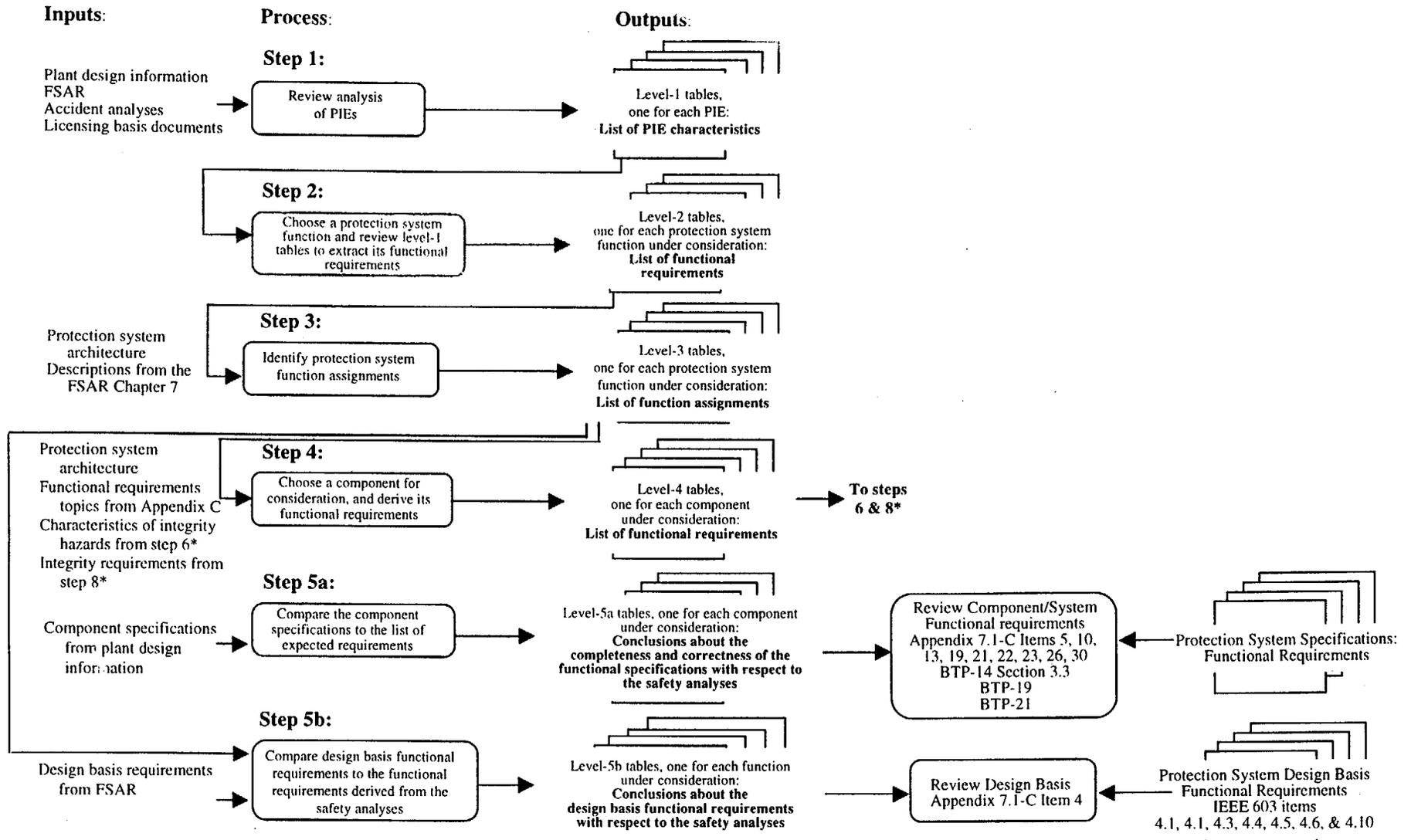
<sup>4</sup> As the Structured Approach is used, a Library of Specification Topics will be built up. These topics collected together become a Requirements Topic Library. As the library grows with each review, a new reviewer can refer to it before developing specific Requirements Topics for the project under review.

<sup>5</sup> Where a reviewer encounters a situation that is not covered in the Requirements Topic Library, the reviewer must define the new topic. (These additions to the library should be retained and made available for use in future reviews. In this regard the Structured Approach also serves as a tool for communicating experience between reviewers.)

<sup>6</sup> Currently SRP Appendix 7.1-C and Branch Technical Positions 14, 17, and 19 cover the review of component and system requirements at a high level.

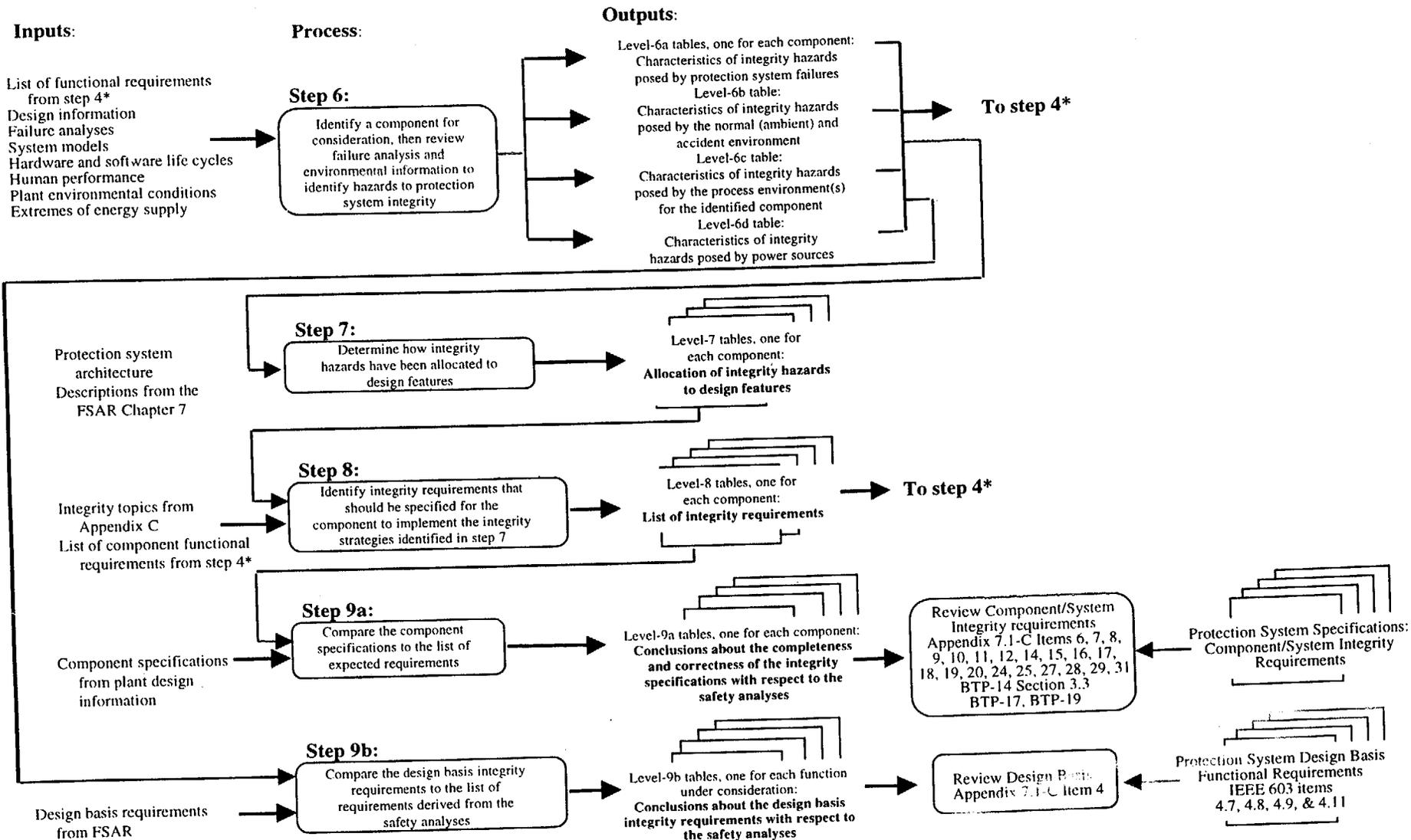
## REFERENCES

- Beltracchi, L., "Notes on a Means-Ends Requirements Hierarchy, Attachment to Statement of Work W6677, U.S. Nuclear Regulatory Commission, November 26, 1996.
- Berg, R.S., Johnson, G.L., "A Structured Approach for Review of Digital Plant Protection System Requirements Specifications," Sandia National Laboratory, June 8, 1998.
- Rasmussen, J., Pejtersen, A. M., Goodstein, L.P., "Cognitive Systems Engineering," John Wiley and Sons Inc., 1994.
- Scott, J.A., "Potential Review Considerations for the Requirements Specification Framework," Lawrence Livermore National Laboratory, CS&R 97-05-11, May 21, 1997.
- Staple, B.D., Berg, R.S., Mahn, J. Forrester, J., Whitehurst, H., "A Total System Requirements Specification Framework for Evaluating Digital Safety Systems in Nuclear Power Plants," Sandia National Laboratory, August 5, 1997.



\*The functional requirements and integrity characteristics interact such that the functional requirements must not create an integrity hazard that cannot be addressed. The functional and integrity requirements must not be mutually exclusive.

Figure 1a. Analytical Steps of the Structured Approach, Steps 1-5



\* The functional requirements and integrity characteristics interact such that the functional requirements must not create an integrity hazard that cannot be addressed. The functional and integrity requirements must not be mutually exclusive.

Figure 1b. Analytical Steps of the Structured Approach, Steps 6-9

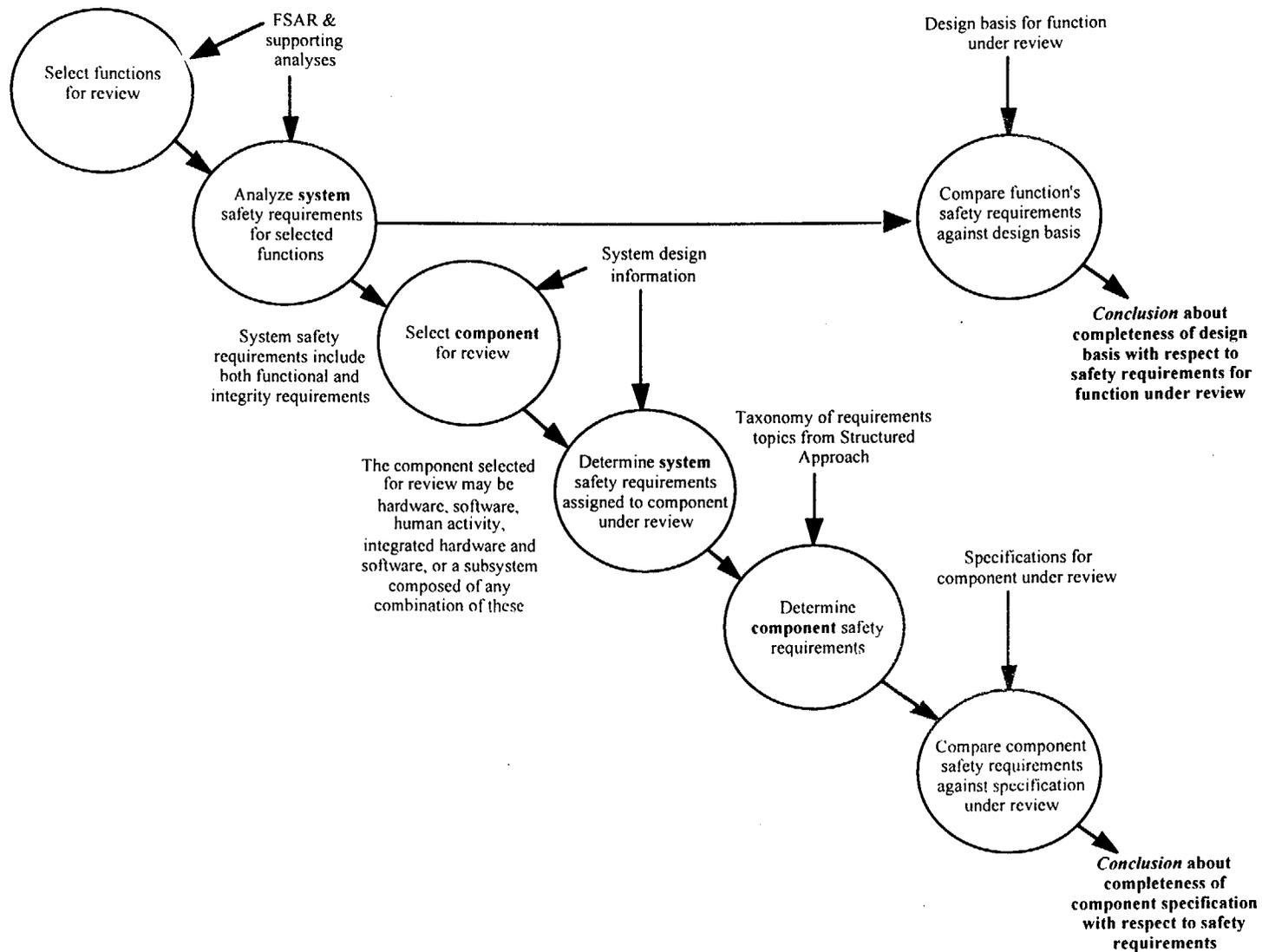
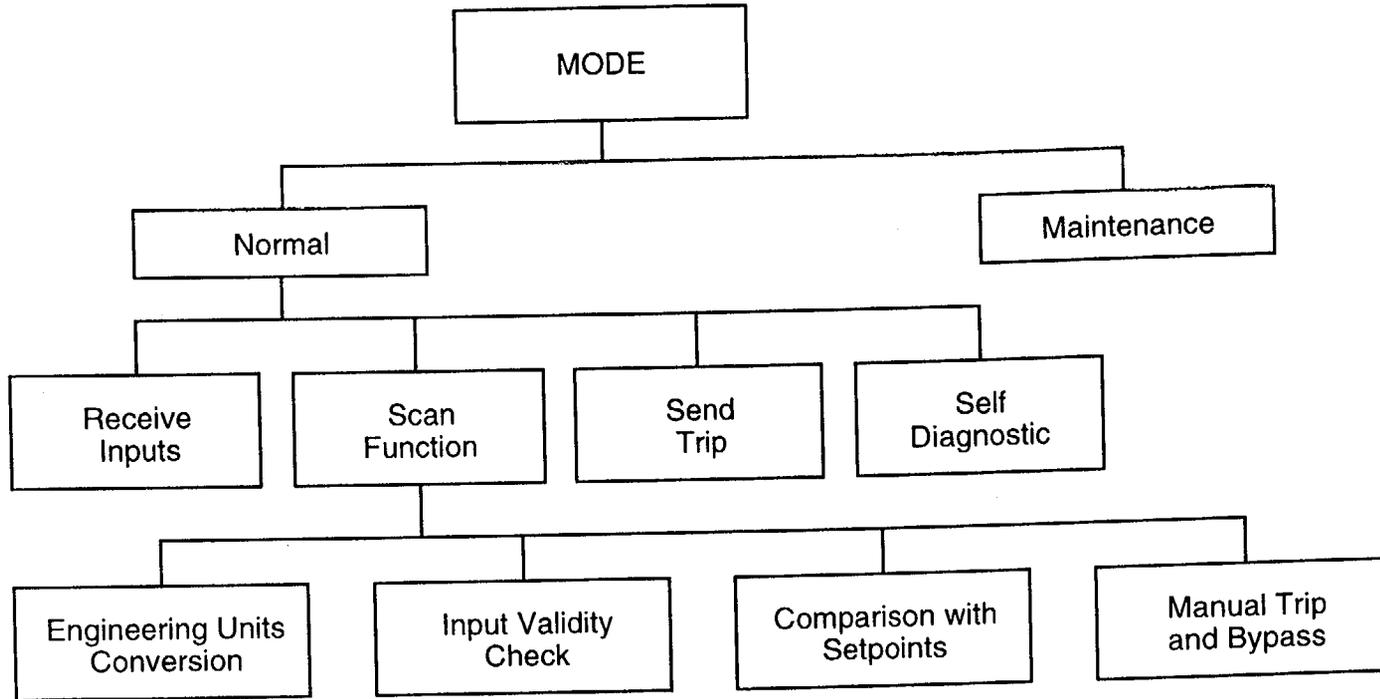


Figure 2. Application of the Structured Approach from the User Perspective



**Figure 3. Hypothetical Structure for a Bistable Trip Device**