International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human-Machine Interface Technologies
(NPIC&HMIT 2000), Washington, DC, November, 2000.

A STRUCTURED APPROACH FOR THE REVIEW OF DIGITAL SYSTEM REQUIREMENTS SPECIFICATIONS FOR NUCLEAR POWER PLANTS[1]

Robert W. Brill
US Nuclear Regulatory Commission
11545 Rockville Pike
Rockville, Maryland 20852
rwb2@nrc.gov

Gary Johnson
Lawrence Livermore National Laboratory
P.O. Box 808
Livermore, California 94551-9900
johnson27@llnl.gov

Keywords: Instrumentation and Control, Requirements Specification

ABSTRACT

This paper discusses the development of a structured approach for reviewing digital systems using a systems engineering technique to extract the requirements from the system level through the module requirements level. The structured approach was tested using the requirements for a Reactor Protection System for an advanced design nuclear power plant. It was found that it supported a very broad review of the requirements and established traceability between requirements and fundamental safety objectives. It also highlighted areas for further investigation which may not be identified in a less rigorous review.

1. INTRODUCTION

Instrumentation and Control (I&C) systems provide monitoring, control, and protection functions in nuclear power plants. 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 which must be considered such as sampling rate considerations, cycle times, discreteness of monitored parameters, greater susceptibility to environmental effects, and computer software quality.

[1]The views expressed in this paper are those of the authors and should not be construed to reflect the U. S. Nuclear Regulatory Commission position.

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 software errors are caused by incorrect or incomplete requirements.

1.1 PROBLEM

Systems engineering methods have not been developed to assure that nuclear power plant 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. Chapter 7 of the NRC Standard Review Plan (SRP) for nuclear power plants[2] 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.

1.2 GENERAL APPROACH

In performing a "thread" audit, the NRC 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. The Structured Approach first addresses the system level requirements, then the module level. The process is similar at all stages.

The Structured Approach is based on the concept that the developer: 1) will have begun with determining the hazards to a Nuclear Power Plant (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.

---

[2]NUREG 0800 Chapter 7 "Instrumentation and Controls" Appendix 7.0-A Review Process for Digital Instrumentation and Control Systems section C.2. Review Process for Software in Digital Instrumentation and Control Systems

In using the Structured Approach, the reviewer derives the requirements expected from NPP safety and system analyses by completing two sets of 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 is collected into one or more tables. One set of tables defines the expected functional requirements, and compares them to actual system design bases and component requirements specifications. The second set of tables defines the expected integrity requirements, and compares them to actual system design bases and component requirements specifications.

1.3 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 Final Safety Analysis Reports (FSAR) , identify the high-level functional requirements (both the functions to be performed and the performance required of those functions) necessary to ensure the integrity of the reactor coolant pressure boundary, to ensure the capability to shut down the reactor and maintain it in a safe shutdown condition, and to 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. 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.

Once the protection system design is known, hazards to the integrity of the protection system itself are identified by analyses of the systems and system failures that can threaten its integrity. The integrity hazards considered include both abnormal conditions and events (ACEs), which include both plant excursions and natural-phenomena-related events that must be handled on a real-time basis by the protection system, and digital development process hazards that must be anticipated in order to avoid introducing errors that could lead to hazards being incorporated in the final design. ACEs thus include hardware failures, software errors, human errors, and environmental hazards. The hazards posed by hardware, software, and human performance are identified so that specifications can be checked to confirm that they include design strategies and features that (1) minimize protection system failures, (2) ensure that the protection system design is robust, and (3) ensure that functional requirements are met when failures occur. These include, for example, requirements for quality, single-failure tolerance, diversity, testability, and independence. Environmental hazards are determined by the envelope of the environment within which the protection system must function under normal and abnormal conditions. This includes, for example, requirements for challenges to integrity

derived from thermal (all sources), pressure, radiation, electromagnetic and radio frequency interference, humidity, power supply variations, seismic, and missile hazards.

Most integrity requirements are evaluated in a top-down fashion starting with Potential Initiating Events (PIEs) analyzed in Chapter 15 of a Final Safety Analysis Report. This top-down approach enhances traceability and minimizes the potential for conflict. The most notable exceptions to a top-down approach are hazards to protection system integrity resulting from specific hardware and software design features, which, because they cannot be identified until the design is specified, must be handled iteratively.

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. Figure 1b shows the last four steps which extract the Integrity requirements.

1.3.1 The First Five Steps: Extracting Functional Requirements

Step 1 The structured approach begins with a review of Potential Initiating Events (PIE) accident analyses to identify protection system functional requirements. This review of PIEs 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 and puts them in step1 tables.

Step 2 The protection system requirements are identified by deriving them from the analyses of these PIEs. By analyzing the information collected in the step1 tables, reviewers can extract the limiting cases that describe the protection system functional requirements for the specific protection system function and puts them in step 2 tables.

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. The subsystem assignment information is then added to the step 2 table that describes the functional requirements for the protection system function under review, to produce a step 3 table. One step 3 table is generated for each protection system function under consideration, so there is a 1:1 correspondence with the step 2 tables.

Step 4 The functional requirements that were identified in steps 1 and 2, and knowledge about the protection system design, is used to develop functional requirements for any specific component that is being

considered for review. The information in the step 3 table of functional requirements is used to create a new, step 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 is strongly dependent upon the component's role in the system architecture. As part of this step, the reviewer uses the Requirements Topics[3] to convert each high-level requirement identified by previous steps into specific requirements for the component under consideration In all cases the functional requirements identified by the analysis in steps 1–3 must be appropriately reflected in lower-level requirements

Step 5a The list of expected requirements collected in the step 4 tables is evaluated against the actual specification for the component(s) under review (step 5a) to create a step 5a set of tables. (These are 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 confidence that the functional requirements in the component specification are reasonably complete, although the process cannot guarantee absolute completeness.

Step 5b As in step 5a, the design basis requirements from the Final safety Analysis Report (FSAR) and the function assignments from the step 3 tables are compared to the functional requirements derived from the safety analyses.(These are the balance of the actual component functional requirements reviews, after all of the pertinent information has been generated in steps 1 through 4 above.)

1.3.2 Final 4 steps: Extracting Integrity Requirements

Step 6 The hazards to protection system integrity are determined by examining safety and system analyses. Information from this analysis is recorded

[3] A Requirements Topic is the description of a specific requirement. E.g., for a sensor there is a requirement to measure a specific range of inputs. The Requirements Topic ,for example, describes the fact that sensor specification must include a requirement describing range of inputs to be measured.

in a set of step 6 tables that identify integrity hazards posed by hardware; software; normal, abnormal, accident environments; and process environments

Step 7 The top-level protection system architecture and FSAR are reviewed to identify how the integrity hazard characteristics, extracted from the step 6 tables, are allocated to the protection system design. This information is then added to the level-6 tables to produce step 7 tables. There is a 1:1 correspondence with the step 6 tables.

Step 8 The hazards to protection system integrity that were codified in the step 7 tables are used to develop step 8 tables that describe the integrity hazards that must be addressed by the particular protection system components selected for review. 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[4] 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 step 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 step 9a set of tables. If an expected integrity requirement listed in a step 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 confidence that the integrity requirements in the component specification are reasonably complete, although the process cannot guarantee absolute completeness.

Step 9b The design basis requirements from the FSAR and the characteristics of integrity hazards from the step 6 tables are similarly compared to the

[4]The Structured Approach for Review of Digital Plant Protection Requirements Specifications: Details - Volume 2 Report provided a catalog of example mitigation and defense requirements specification topics that are typically important for the sense, command, and execute features of protection systems.

integrity requirements derived from the safety analyses. 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.

2.0 STRUCTURED APPROACH TRIAL

The Structured Approach discussed in the previous section was tested on a Advanced Boiling Water Reactor protection system. The intent of the test was evaluate the completeness of the Structured Approach and its potential usability as a requirements review tool.

The trial application of the Structured Approach demonstrated the following:

1. It supported a very broad review of protection system requirements and established traceability between requirements and fundamental safety objectives. It also highlighted areas for further investigation which may not be identified in a less rigorous review.

2. The trial found the need to review a very large number of plant design documents in order to obtain the necessary information.

3. The use of the Structured Approach for a complete review takes a lot of effort, and would have to be refined more to be efficient for an NRC reviewer. For a thread analysis, however, the methods are adequate.

4. The Structured Approach collects insufficient data regarding exactly what functions must be performed. Rather, it generally identifies the functions but does not specify the specific functions required of protection systems functions. This is because plant documentation does not contain this information. The design function adds the specificity to the general functions.

5. At this time, 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. This is because this is a design function which is performed after the plant documentation has been reviewed.

6. The Structured Approach led to the concept of developing a set of review templates for the steps that can be used by NRR staff in

reviews. The templates will be an effective practical use of the structured approach.

7. The major benefit of the Structured Approach is that it gives the reviewer a thorough understanding of the basis for the design.

3.0 CONCLUSIONS

The Structured Approach provides a systems engineering approach to performing a top down traceability from systems requirements through software and hardware requirements specifications. For example, 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 could exist 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 bi-stable module then decomposes into a standard set of sub-modules.

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.

The structured approach needs further refinement, but it is a repeatable technique that can establish traceability from system requirements through software requirements.

ACKNOWLEDGMENTS

Leo Beltracchi
Ray Berg, Sandia National Laboratories
John Calvert, US Nuclear Regulatory Commission

REFERENCES

A Structured Approach for Review of Digital Plant Protection System Requirements Specifications: Overview - Volume 1; Ray Berg, Sandia National Laboratories; Gary Johnson, Lawrence Livermore National Laboratory; Robert W. Brill, Nuclear Regulatory Commission; August 31, 1999 (USNRC Public Document Room - ADAMS Accession Number MLl003712504)

A Structured Approach for Review of Digital Plant Protection System Requirements Specifications: Details - Volume 2; Ray Berg, Sandia National Laboratories; Gary Johnson, Lawrence Livermore National Laboratory; Robert W. Brill, Nuclear Regulatory Commission; June 15, 1999 (USNRC Public Document Room - ADAMS Accession Number ML003712531)

A Structured Approach for Review of Digital Plant Protection System Requirements Specifications: Trial Application to Advanced Boiling Water Reactor Protection System Requirements - Volume 3; Gary Johnson, LLNL; Ricardo Yamamoto, UC Berkeley, August 31, 1999 (USNRC Public Document Room - ADAMS Accession Number ML003712751)

NUREG-0800, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants; US Nuclear Regulatory Commission; September 1997

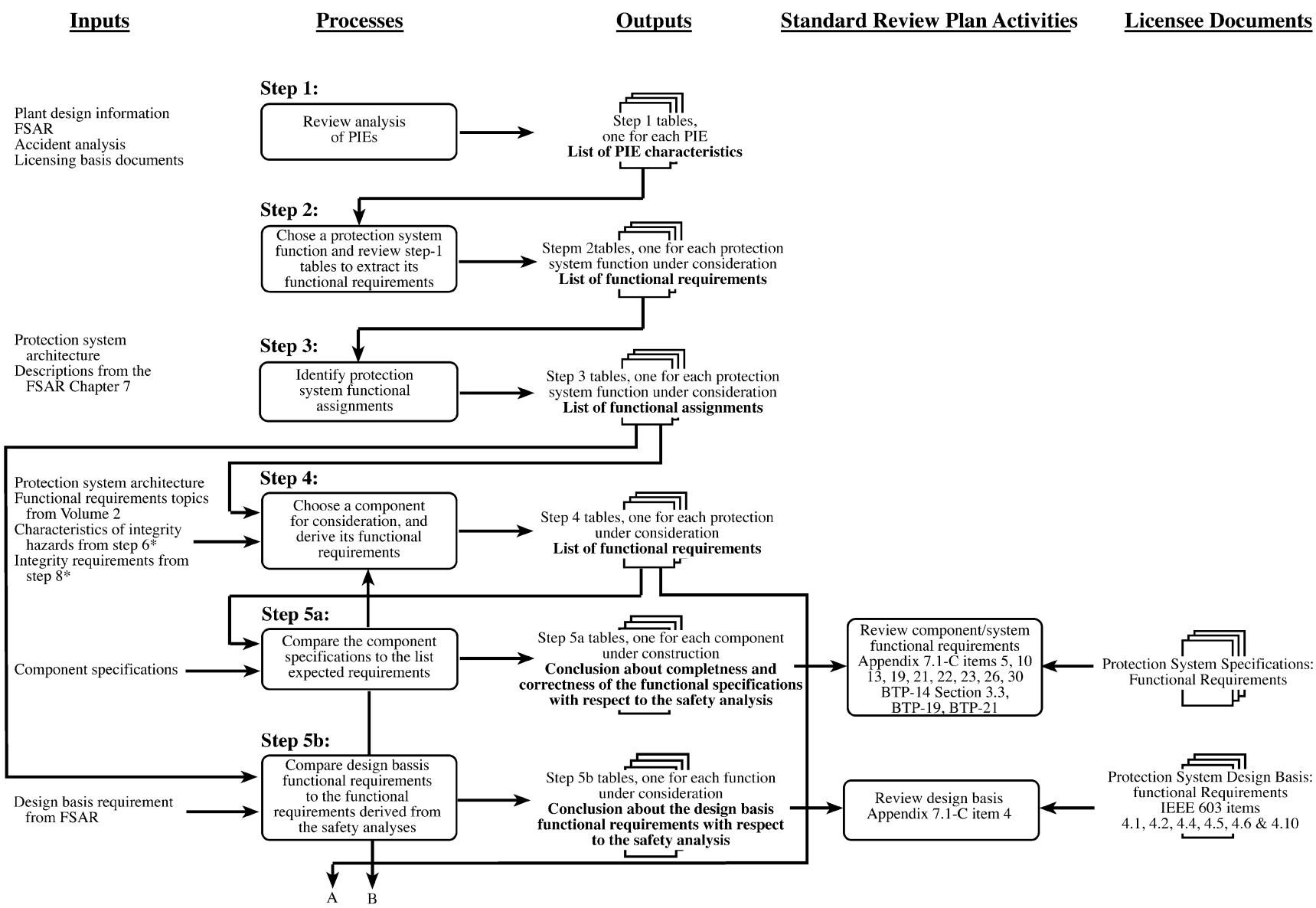

Figure 1a The First Steps: Extracting Functional Requirements

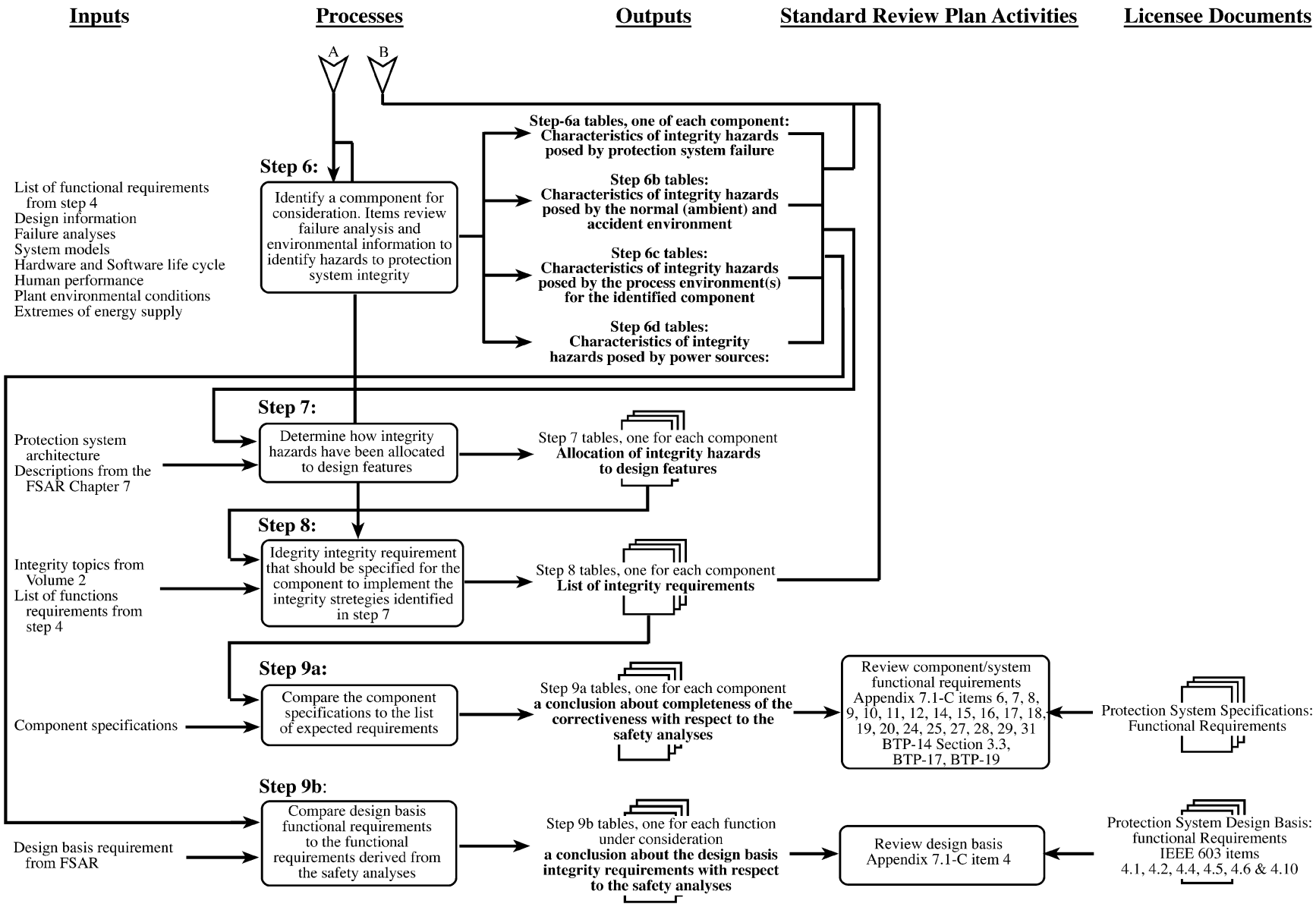

Figure 1b The Last 4 Steps: Extracting Integrity Requirements