Design Reliability Engineering and Its Application As Design Integration Tools
설계 통합 도구로서의 하드웨어 설계 신뢰성 공학 및 그 응용

Y. S. Kim*
김 연수
Y. B. Chung*
정 영배

요 지

하드웨어 설계 과정에서 신뢰성 담당자들에게 당면한 문제는 요구된 임무에 필요한 기능적 요구사항의 달성 가능성과 요구된 임무를 달성할 확률의 예측여부 및 이의 적합성을 판단하는 것이다. 첫번째의 문제는 기존의 신뢰성 공학의 방법을 사용하여 해결되지만 두번째의 문제는 잦은 사후 설계 변경을 필요로 하기 때문에 항상 시스템 전체에서의 최적을 고려하여 이루어지지 못하고 있다. 본 논문에서는 그러한 잦은 사후 설계 변경등으로 인한 취약한 점을 극복하기 위한 방법론으로 하드웨어 설계 신뢰성 공학을 다루며 그 분석 도구로서 목표달성 나무(Goal-tree)의 사용과 그 응용을 제시하고자 한다.

1. Introduction

Our products or processes which are able to deliver the customer-demanded performance in the short-term as well as the long-term, sustained performance are necessity to our current world-wide competeting market. Reliability is a critical characteristic which measures sustained product-process performance. Also, maintainability measures sustained product-process support. Reliability and maintainability characteristic must be defined, designed, and manufactured into each product that we deliver to our customer (Kolarik).

The reliability and maintainability of product or process is strongly influenced by decisions made during the design process. Reliability and maintainability needs and expectations that inherent in customer demaneds must be translated into long-term sustained performance as earlier as possible during design process. It is essential that systematic design disciplines are used which minimize the possibility of failure and which allow design deficiencies to be detected and corrected as early as possible. The design must also take account of all possible factors that can affect reliability and maintainability such as manufacturing conversion process, operating condition and exposed environment, maintenance and failures not caused by load. Though a life testing is often needed for establishing that a product or process meets the reliability and matainability goals, invariably life testings are an enormously expensive way of measuring the effectiveness of

* Department of Industrial Engineering, University of Inchon

a design idea in improving the product/process reliability and maintainability. The following questions would be constantly answered by reliability engineers under the banner of reliability improvement or design for reliability: How to develope a reliable system in a short time and make the system cost less ? How to cut down the high cost and long time presently needed for reliability and matainability measurement ? Do we still have high .confidence in the measurement data?

The starting point of designing reliable products or manufacturing processes in such cases involves:

1) Using the institutional knowledge base about the scientific principles and engineering experience
2) Generating new engineering knowledge.

Efficient, error-free implementation of the institutional knowledge base can be achieved throgh the use of modeling, check lists, databases, and computer expert systems.

The point to address at this point for design-in reliability and maintainability into products or processes are: 1. We have many available techniques to apply. 2. It is necessary to assemble all the available resources systematically in order to achieve very reliable design-in process at the beginning of development process both in qualitatively and quantitavely. 3. Design reliability engineering along with Goal-tree technique has practical advantages over the traditional method. The key to such successful system design, development, and implemenation lies in treating all of the system and support system design consideration in the context of their contributions to overall system performance throughout its intended life cycle, as functions of qualitive and quantive measures in the early process of its process. These considerations include the user-defined performance requirements, planned usage conditions, and how the system will be operated and supported. Figure 1 illustrates the interactions among the system reliability, maintainability, and support system design characteristics which must be considered during the system design engineering and development process to achieve the required system-level performance levels. System level requirements are developed by the users and form basis for system design activities (RMS Guide book).

During hardware design process, the issues with which we would be confronted are: 1) Will hardware meet all mission functional requirements (capabilities)? 2) Is the probability of mission success predictable and is it acceptable? Issue 1) is usually routinely resolved and satisfied by the methodologies of current reliability engineering, but issue 2) is often resolved post design, i.e., afterwards design completed and is not always an integration part of system hardware optimization. This post design weakness is the one which requires our attention.

In order to overcome this weakness, Design reliability engineering can integrate design process, reliability analysis techniques, and expert systems to achieve very reliable, minimum-cost hardware. As a analysis tool, GTA technique provides practioners a means to start with.

The purpose of this paper describes the design reliability engineering approach that is considered to be helpful in reliability improvement efforts and discuss the GTA techniques and procedures as an implementation vehicle for design reliability engineering.

2. The Design Reliability Engineering Approach

To meet the challenge of cost effective design, improved techniques will be required to achieve the high reliability and maintainability requirements. The frame work of a design process exist that can be build on integrating the best features of design, reliability and maintainability engineering and analysis, and expert systems. A key element in the approach is the systematic development of the methodology and incorporating standard building blocks into computerized models. The steps to perform the design reliability approach are evolving and will require experience to achieve the desired goals. Figure 2 shows the steps necessary to the design reliability engineering process. Those steps are as follows:

1) Start with a clear and unambiguous definition of the mission objectives and constraints.
2) Derive the necessary individual hardware functional objectives directly from the mission objectives and constraints, to ensure complete integration of all aspects of the design.
3) Identify the performance of each functional system element on the basis of quantitive estimates of their relative importance.
4) Develop conceptual designs for the functional elements.
5) Develop component behavior models and include an evaluation of the uncertainties within models. The models needed to include validation measures based on both analytical and test data.
6) Use modeling uncertainties and uncertainties associated with materials, fabrication, assembly, and other variables to design individual components.
7) Perform sensitivity analysis to identify the key variables in the design and to use them as a basis for testing and validation programs.

For the first three blocks illustrated in figure 2, figures 3 and 4 illustrate the design reliability engineering process. The first step is a clear, concise statement of the mission objectives. The example uses a space nuclear power plant that must operate unattended for many years with a high probability of providing rated power at the end of mission. From the mission requirements, functional requirements are derived. Only one path is followed in the illustration. This continued in figure 4 where on finally reaches the level of functional element requirements. The transition to hardware and conceptual design can be now begin. The process is systematic and requires much tedious detailed analysis. However, it forces one to think of all aspects of the design before plunging into design decisons.

3. Design Integration Tools

GTA is utilized to identify success paths, or success trees, that lead to the fulfillment of a specific reliability goal. It focusses not on a specific fault event, but rather on a specific system goal or objective. It guides to the construction of a logic diagram of all conceivable event sequences (incluing both physical and human) which could lead to the achievement of the goal event. The Goal-tree means a graphical representation of various combinations of goals, subgoals, equipment, or system sucesses that rulst in the success of the top event (Roush et al.). Goal-tree is develped with aid of Boolean logic operator. Those are AND, OR or other gate logic structure to show the relationships of subgoals that produce the main goals. The goal tree is developed backward until the system goal is achieved in terms of the systems components. A Goal-tree is developed using the steps below:

1) Identify the system goal at top of the tree.
2) Identify the subsystem successes path that could lead to the top event.
3) Determine the logical relationships between the goal, subgoals, and functions.
4) Identify system success path using logic gates.
5) Quantify the Goal-tree.

Figure 5 depicts a partial development example of Goal-tree.(Kolarik).

When Goal-tree system relationships of main interest are developed, it could identify and fully aware of faulty and weak design points and narrow down to the cause and effect relationship of main concern. As the following step, Quantified results could be generated utilizing computer models based on similar case of past experience or case. Then, design decision trades about whole lifecycle of products or processes are speculated.

Development of the Goal-tree models for systems and components not only provide the design basis descriptions but also implicitly contain very detailed cause consequence descriptions of how the hardware suceeds and fails. This means that test program developer is able to fully examine potential failure paths, the intermediate damage states which result from failure propagation and identify the information which would be emitted if that failure propagation paths were active. This means that the informational needs for inferring the internal condition of hardware during its operation can be defined a priori , and that comprehensive non-destructive testing program can be defined to determine the rates of progression for many importantfunctional failure modes. The Goal-trees for hardware tend to be generic and merely needed to be tailored for a specific application, so it is feasible to construct an expert database which could be interactively used by future designers to build and specify comprehensive hardware testing programs.

4. Iteration Process and Sytem Integration

Simulation and logic models which have greater realism, detail and complexity than those developed for the conceptual design are used to examine the relationships between the capacity and reliability of individual components, system geometry and dynamic character, local and global environment effects and the overall reliability structure of the design. These influences on performance are selectively varied so that the worth of enhancements, alternate schemes or differing levels of hardware capacity can be compared and the best combinations identified. When the prototypical hardware is proposed and there is little or no empirical evidence from which to infer future performance levels or failure probabilites, the designer must describe the uncertainty in hardware performance with probabilistic distributions. The effect of this uncertainty on overall system performance must be described in a like manner.

The value in using design reliability engineering approach is that the areas of greatest uncertainty and importance can be addressed early in the design so informed guidance for selection of design hardware is available and subsequent maturation of the design occurs as quickly as possible. A computer expert programs could assist the designer in interactively defining the appropriate probablistic information required for each model by either providing built-in heuristic relationships or expert deep knowledge data bases.

The designer will iterate between the tasks identifed above using combinations of thermal-hydraulic, finite elements (stress) and reliability models and simulations to determine and compare the relative worth of proposed changes with the benefits which result from improved mission or life-cycle costs. The process will continue until the solution is optimal.

As the reliability of individual systems increases, dependent system faults and common cause failure mechanisms become more important. The nature of these dependencies requires that they not only be rigorously identified, but that they be fully integrated with the system models to establish their importance to maintain overall mission success. This concern with dependent systems, such as cooling, motive power and controls, and with common cause failures that result from inter-spartial relationships and common hazard vulnerabilities leads to the need for dedective approaches such as fault tree analysis. It is through these fully interconnected models that the reliability engineer takes on the role of a systems integrator and ensures that inter-system boundaries are compatible and exhibit adequate overlap. By encouraging the designer to interactively estimate the important situation-specific influences on stress and material strength, the domain over which they are likely to range, and their functional relationships, it should be possible to synthesize probabilitic load strength relationships. This will provide the designer with a means of estimating failure probabilities for passive component for which their is usually no data and in some cases active prototype components. Achieving these interactive capabilities requires that the software contain the expert descriptions of the influences on material strength and loads and all the functional relationships between them - in other words, an expert description of the mechanisms by which classes of components succeeds and fail. Goal-tree analysis can be an effective tool in achieving definition and understanding of the relationships.

5. Conclusions

The basic tools for designing reliability into high technology systems exists. The practically of doing so in doing in significantly greater detail can be performed with advent of new computers and computer programming technology. This paper has provided some examples of a rationale, an approach and the methods and techniques which are available to the designer to fully integrate reliability into design in the early phase of its lifecycle. This approach is cost effective when one considers the savings in avoiding resign and ability to direct scarce resources to the really critical issues in the design. Their potential benefits are: 1) minimizes need for future redesigns by considering all design aspects from initiation of design process 2) critical components, design parameters, and uncertainties identified early 3) value of reducing uncertainties quantified 4) use of expert systems systematically builds on past experience 5)supports many development facets (design, safety, reliability, test engineering, training, maintenance)

References

1. M. C. Roush el al., Integrated Approach Methodology: A Handbook for Power Plant Assessment, SAND 87-7138, Sandia National Laboratories, Albuquerque: 1987.
2. Society of Automotive Enginners, Inc., Reliability, Maintainability & Supportability Guidebook, Warrendale, PA, 1990.
3. W. J. Kolarik, Creating Quality: Concepts, Systems, Strateggies, and Tools, McGraw-Hill, 1995.
4. W. J. Kolarik, Reliability in Design Class Notes, Lubbock, Tx, 1990.
5. P. D. T OConnor, Practical Reliability Engineering, 3rd Ed.,John Wiley & Sons, 1991.

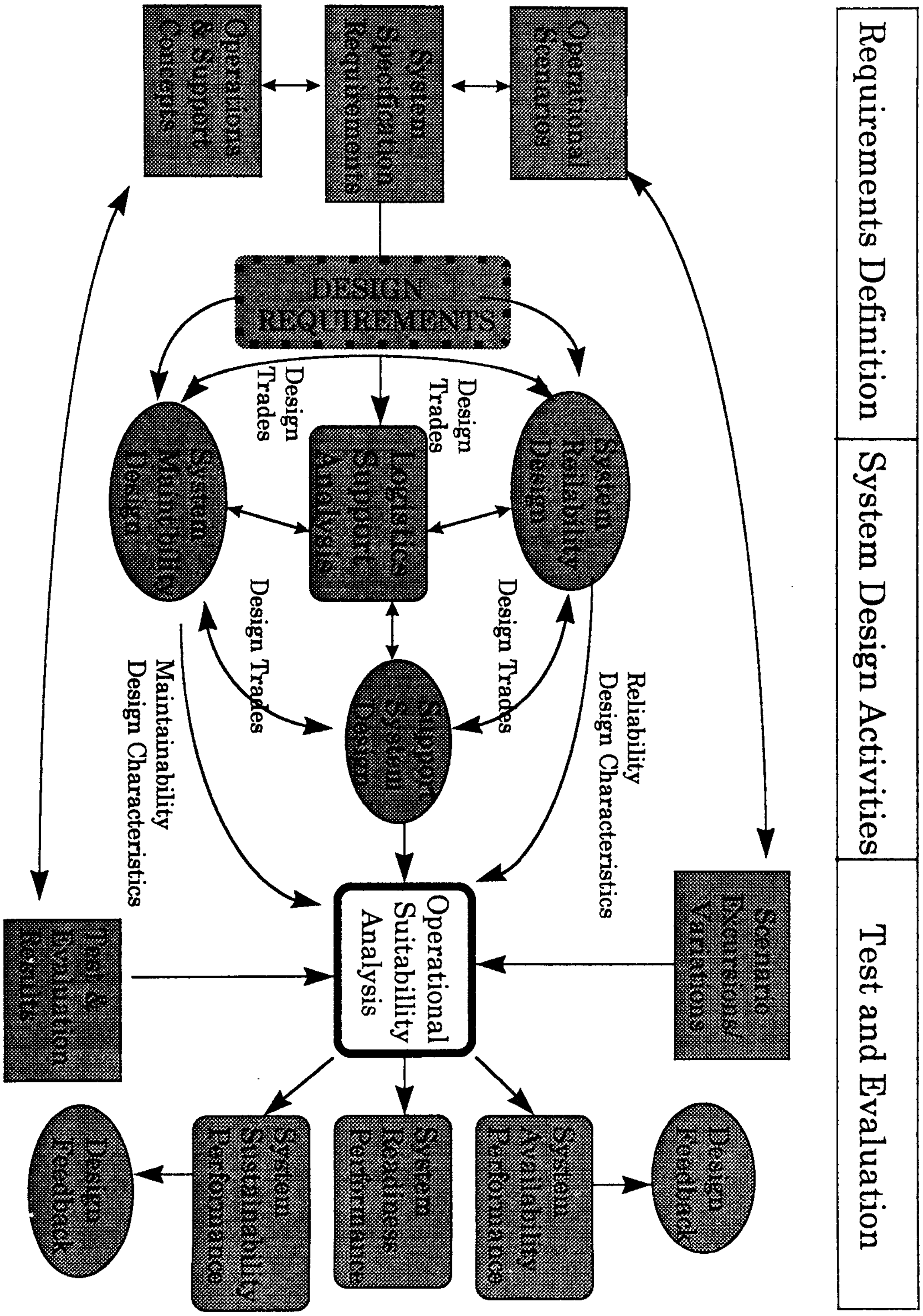
Requirements Definition
System Design Activities
Test and Evaluation
Operational Scenarios
System Specification Requirements
Operations & Support Concepts
DESIGN REQUIREMENTS
Design Trades
Design Trades
System Reliability Design
Logistics Support Analysis
System Maintainability Design
Design Trades
Design Trades
Support System Design
Reliability Design Characteristics
Maintainability Design Characteristics
Scenario Excursions/ Variations
Operational Suitability Analysis
Test & Evaluation Results
System Availability Performance
System Readiness Performance
System Sustainability Performance
Design Feedback
Design Feedback

Figure 1: System Reliability, Maintainability and Support Sytem Design Relationships
(RMS Guidebook)

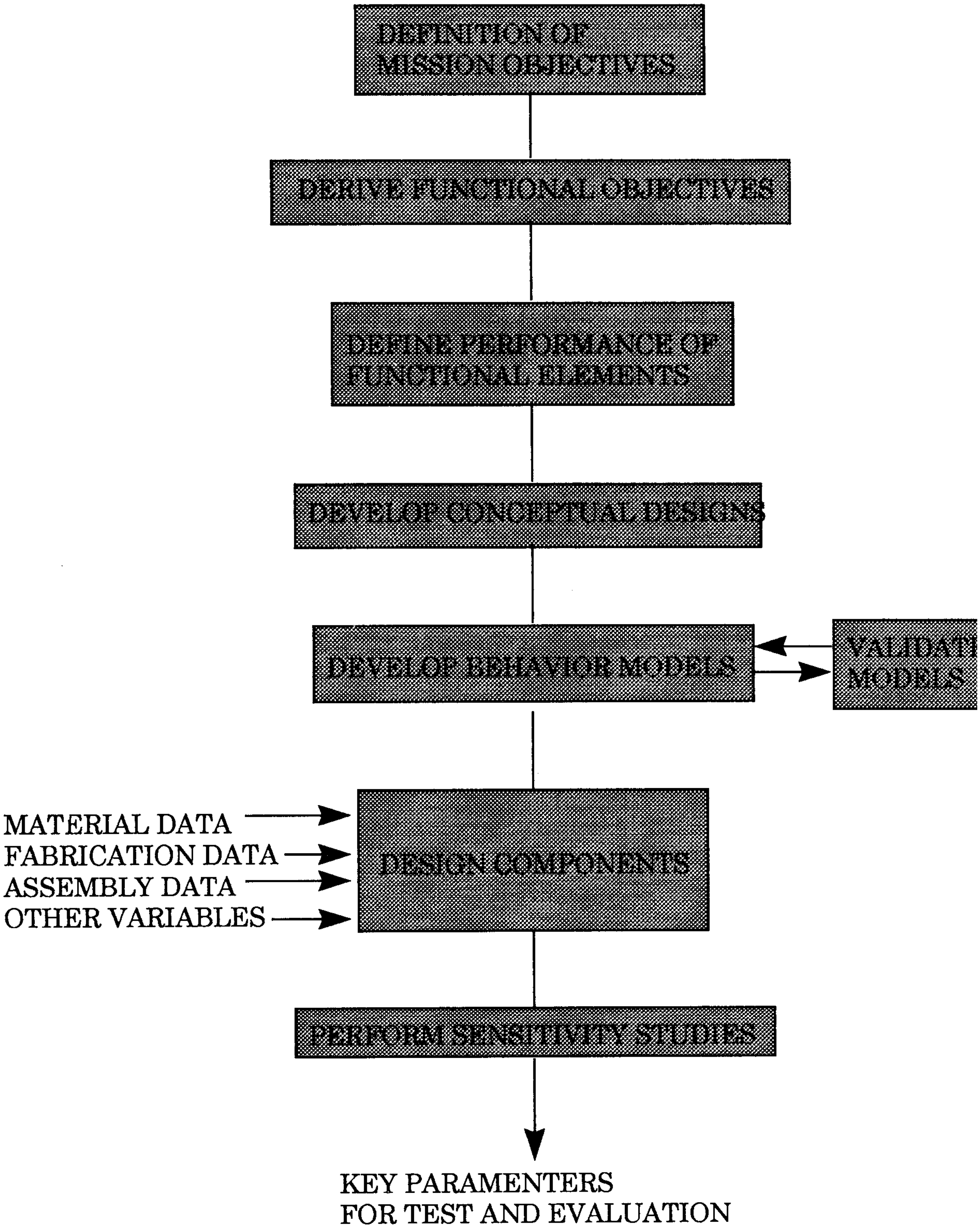

Figure 2: Steps in Design Reliability Engineering Process

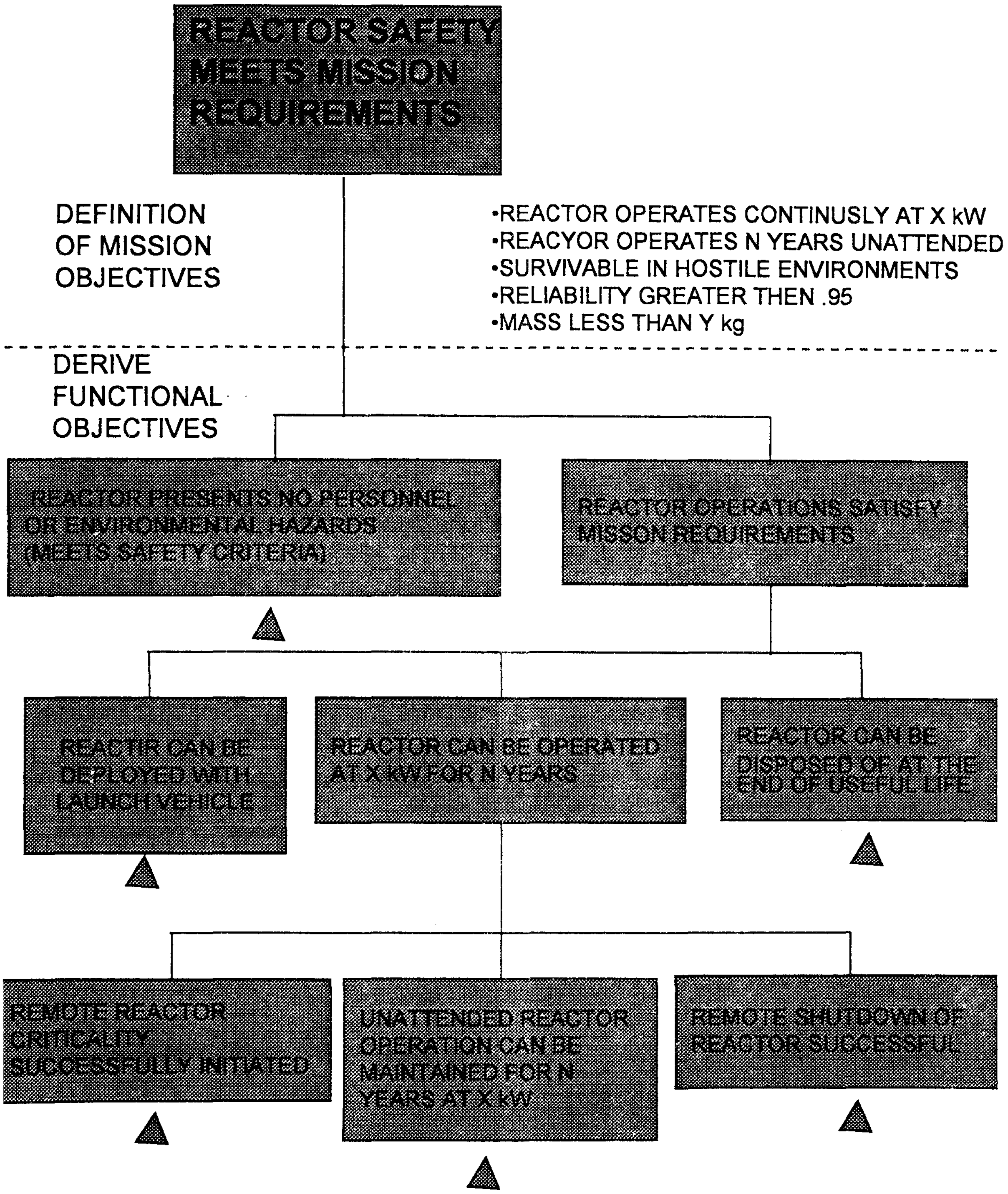
REACTOR SAFETY MEETS MISSION REQUIREMENTS
DEFINITION OF MISSION OBJECTIVES
•REACTOR OPERATES CONTINUSLY AT X kW
•REACYOR OPERATES N YEARS UNATTENDED
•SURVIVABLE IN HOSTILE ENVIRONMENTS
•RELIABILITY GREATER THEN .95
•MASS LESS THAN Y kg
DERIVE FUNCTIONAL OBJECTIVES
REACTOR PRESENTS NO PERSONNEL OR ENVIRONMENTAL HAZARDS (MEETS SAFETY CRITERIA)
REACTOR OPERATIONS SATISFY MISSON REQUIREMENTS
REACTIR CAN BE DEPLOYED WITH LAUNCH VEHICLE
REACTOR CAN BE OPERATED AT X kW FOR N YEARS
REACTOR CAN BE DISPOSED OF AT THE END OF USEFUL LIFE
REMOTE REACTOR CRITICALITY SUCCESSFULLY INITIATED
UNATTENDED REACTOR OPERATION CAN BE MAINTAINED FOR N YEARS AT X kW
REMOTE SHUTDOWN OF REACTOR SUCCESSFUL

Figure 3: Illustration of Design Reliability Engineering Process

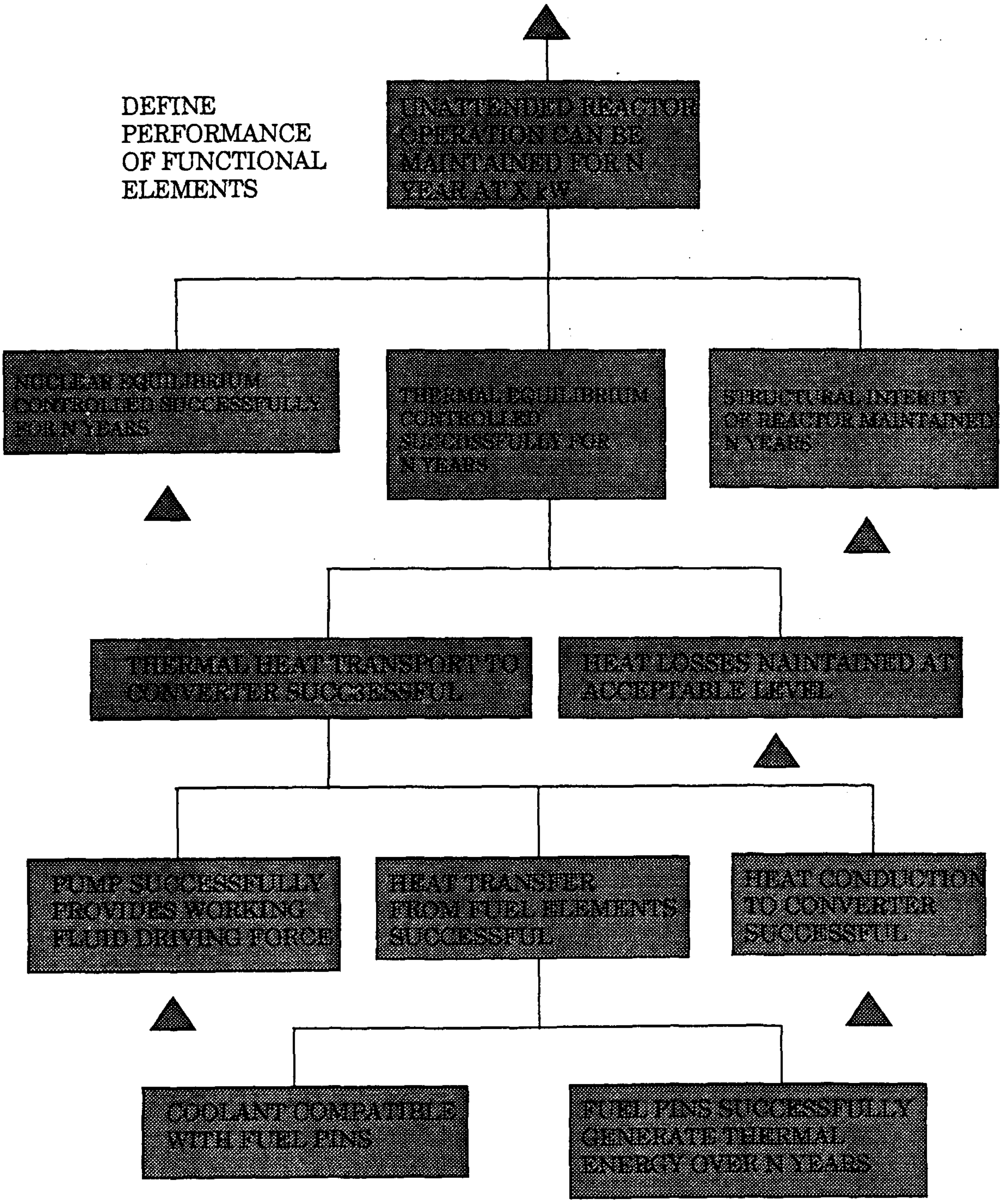
DEFINE PERFORMANCE OF FUNCTIONAL ELEMENTS
UNATTENDED REACTOR OPERATION CAN BE MAINTAINED FOR N YEAR AT X kW
NUCLEAR EQUILIBRIUM CONTROLLED SUCCESSFULLY FOR N YEARS
THERMAL EQUILIBRIUM CONTROLLED SUCCESSFULLY FOR N YEARS
STRUCTURAL INTERITY OF REACTOR MAINTAINED N YEARS
THERMAL HEAT TRANSPORT TO CONVERTER SUCCESSFUL
HEAT LOSSES NAINTAINED AT ACCEPTABLE LEVEL
PUMP SUCCESSFULLY PROVIDES WORKING FLUID DRIVING FORCE
HEAT TRANSFER FROM FUEL ELEMENTS SUCCESSFUL
HEAT CONDUCTION TO CONVERTER SUCCESSFUL
COOLANT COMPATIBLE WITH FUEL PINS
FUEL PINS SUCCESSFULLY GENERATE THERMAL ENERGY OVER N YEARS

Figure 4: Illustration of Design Reliability Engineering Process (continued)

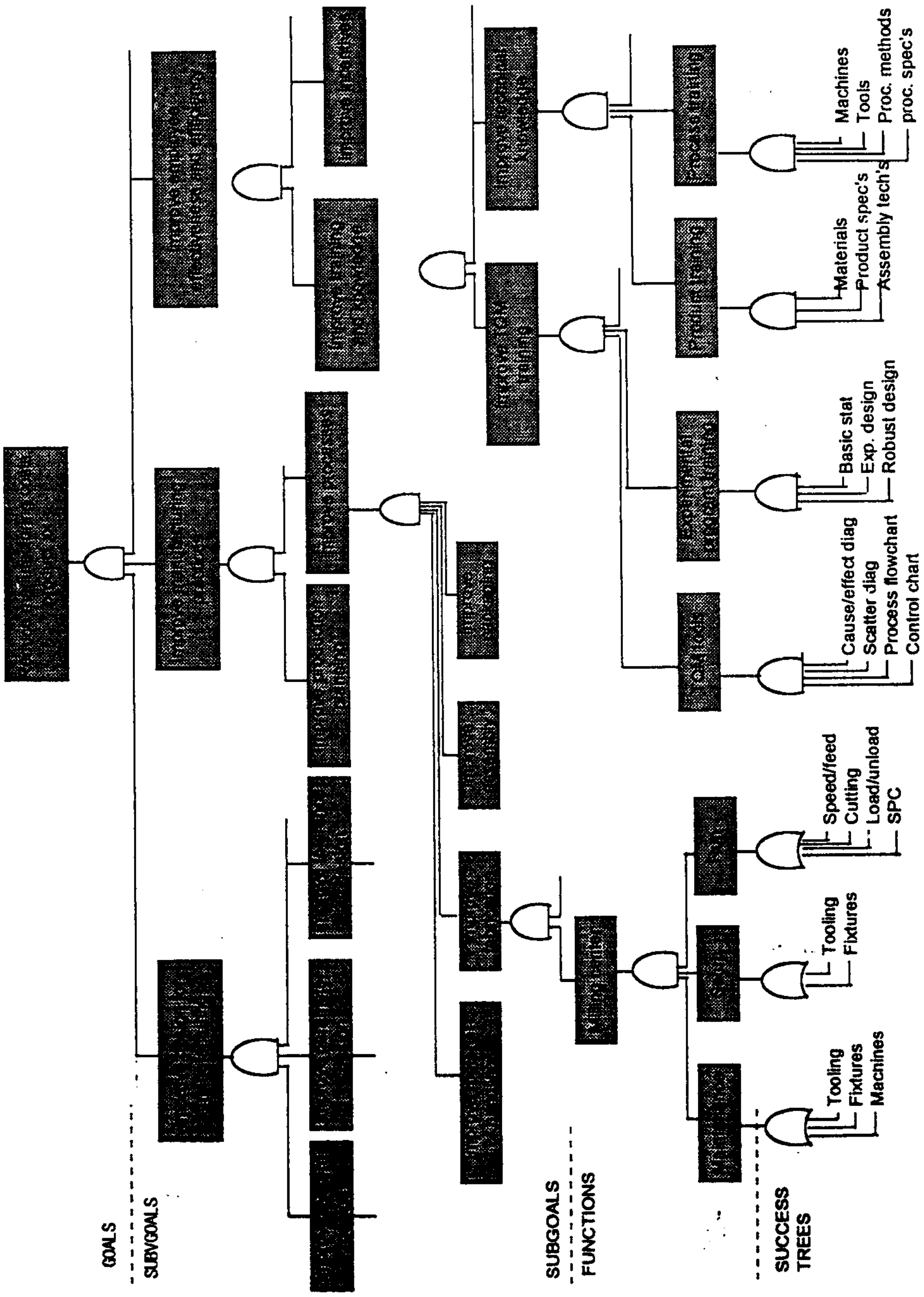

Figure 5: Example of Partial Goal-tree development (Kolarik)