Chapter 4

Problem Formulation and Solution Strategies

The formulation of the research problem, based on the extensive literature review ascribed in the previous chapter, and various planned solution strategies for the identified problems is presented in this chapter. In this chapter issues of analysis for early prediction of safety of a system in dealt with of existing approaches for safety brought out in the previous Chapter 3. Further, the uncertainties, along with their treatment, in early prediction of system safety are considered here and the solution strategies for the quantification of the stated limitations in Chapter 3, regarding the early prediction of system safety, are also addressed.

4.1 Introduction

Safety Critical Systems have Instrumentation and Cotrol(I&C) as an important part. The I&C systems are widely based on hardware as well as software in today's era and failure of any of them is the cause of most system's problem todays. Failures occur because of the presence of fault in system (hardware or software). Furthermore, safety assurance or assessment attempts to study, characterize, measure, analyze the failure and repair (in case the system is repairable) of the systems. This study can be used in order to increase a quality and longevity of a system and minimizing the catastrophic failures. The early assessment of system safety is an effective strategy for the management of risk. Therefore, it can be used in decision making for safe, economical, efficient design and operation of safety critical computer based systems like medical systems, aeronautical systems, NPPs and defense systems.

There are six phases in Safety Critical System Development Life Cycle (SCSDLC) namely: 1) requirements analysis, 2) system design, 3) implementation, 4) testing, 5) deployment and 6) maintenance. Of the six phases of SCSDLC three of them namely requirements analysis, system design and testing are the vital tasks. The fault in any of these phases may lead to an unsafe product, which can lead to catastrophic disasters. The fault can get embed in any of the vital phases of SCSDLC, and hence, there are some techniques through which system's safety can be assured in all these phases. Typical procedure to compute the safety estimates is shown in Figure 4.1.

In spite of potential benefits of these approaches [112], [120], [123],[126], [130], [131], [133] the uncertainties associated with models, parameters, phenomena and assumptions put limitation on its usage in the industries. From literature survey conducted by us, we conclude the following necessary requirements that need to be addressed. These requirements lie in the scope of three important phases of SCSDLC as stated above. Researchers, academicians, practitioners, and engineers are continuously proposing various models for safety prediction of system during architectural design. The existing safety models, at the level of architectural design, use an analytical approach that is incapable of generalizing the quantitative safety analysis methodology. Existing models for safety analysis have problem in identifying failures and hazard segregation. Further, the mapping restriction for all hazards to state space model is involved in such models, the current Computer Based Systems (CBSs) are capable of handling it and need not follow such restriction, which impact on accuracy of the safety estimates of the system. Since, the cost of failure of Safety Critical System (SCS) is very high, therefore, such error of estimated result of safety analysis is strictly prohibited.

Further, the existing models [126], [131], [133], [135] to propose for safety prediction of system during architectural design are based on the state space model. There is randomness or uncertainty of input data/parameters/state variables involved in state space safety models. These uncertainties include the verification of incorporation of all the requirements in the model, verification of the correctness of the model itself even after all the requirements have been taken care of.

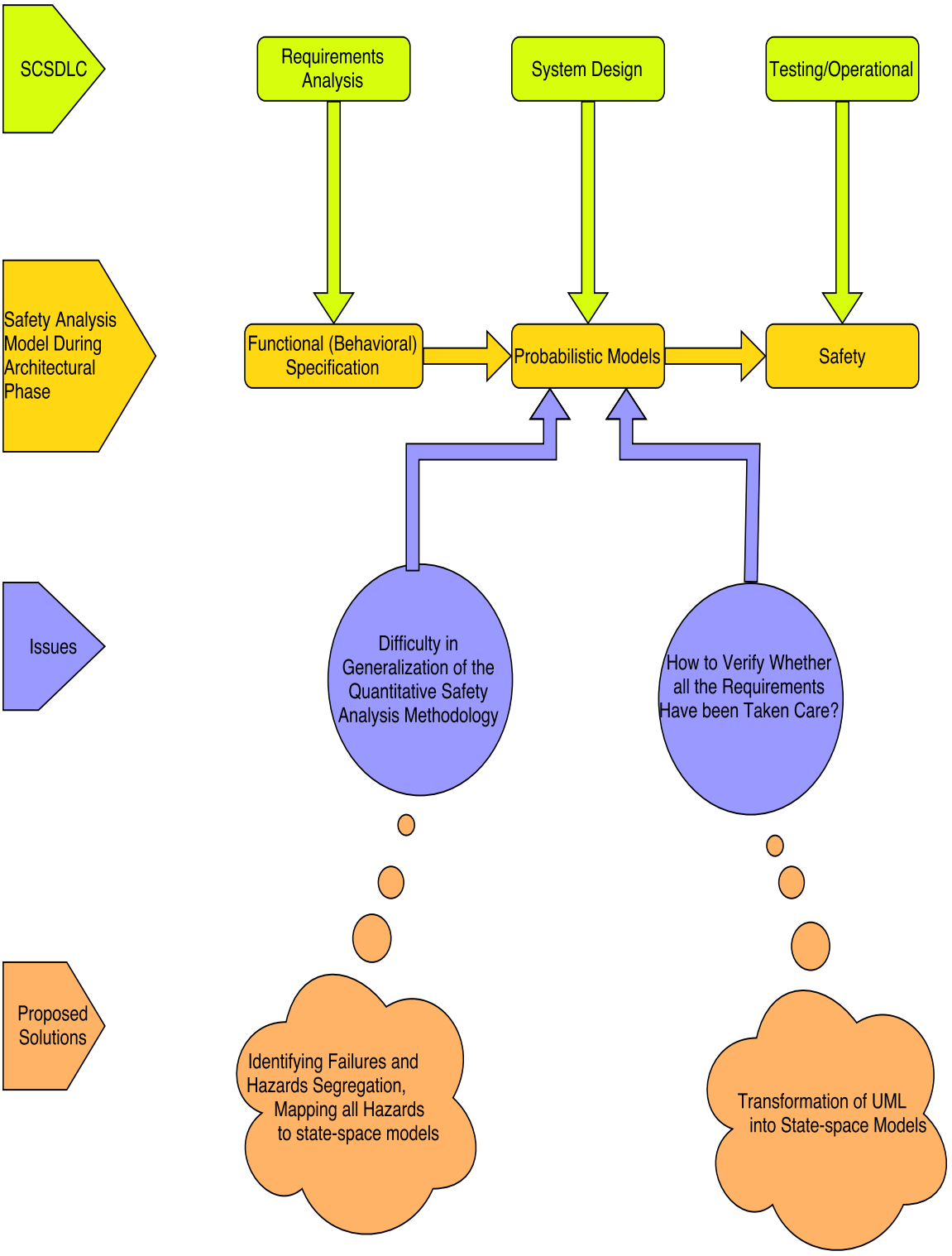

FIGURE 4.1: Issues and proposed solutions for uncertainty in probablistic models of SCS's safety and its estiates

4.2 Problem Formulation

The issues that are identified during different stages of SCSDLC, for probabilistic models of safety assessment of a system need proper treatment to ensure the safety of the system. After literature review regarding the safety prediction, the research problem in this thesis work is two folded as shown in Figure 4.1 and will be explained in the subsequent sections.

4.2.1 Difficulty in generalization of the quantitative safety analysis methodology

In the existing approaches for safety analysis, we found that each approach either assumes probabilities or rely on analytical solvable model to quantifying safety that are difficult to generalize. The one of the limitations of existing approaches [112] is that they only consider hardware failures whereas, an SCS is comprised of hardware and software both and failure of any one of them may lead to system failure. Further, some of the approaches [112], [120], [123] have limitation in terms of selection of Markov model as modeling technique. The limitations of Markov model are as follows:

1. Analysis based on the Markov chain is typically limited to modeling the probability of changes in a system with exponential distribution. However,

processes pertaining to safety may or may not have nature of an exponential distribution.

2. The Markov chain may suffer a state explosion problem that may be difficult to address.

3. The Markov chain is not appropriate to model properties common in a software system such as parallelism, concurrency and multithreading.

Various methods use Markov models for deriving the safety metrics. These methods assume that the failure rates of the some components are zero [123] and treat them as perfect components during the lifetime of the system, which again may be a hypothetical assumption that may lead to a severe accident in case of SCS. In the paper [125], the authors applied a method to quantify certain parameters, which are associated with safety, but, the proposed safety parameters are not validated experimentally. In the paper [130], [132], authors discussed about a qualitative assessment of safety which works in a fruitful manner on non-critical systems, where reliability and safety requirements are not very stringent. The verification is done using PN, although, defining the safety contracts in mathematical form remains a very cumbersome process, especially in complex systems. In the paper [134], authors focus only on identification of hazards sequentially, however, concurrent hazards are possible in case of SCS. Some other approaches [78], [134] use FTA, where in reconfiguration of a system after the detection of failure or system recovery is not possible.

Most of methodologies discussed above are based on either qualitative or quantitative approach to safety analysis, where the applicability is restricted to logically feasible models. However, these quantitative safety analysis methods are difficult to generalize. Therefore, there should be an early safety prediction method to model various possible SCS.

4.2.2 Uncertainty in State-space models

System faults are likely to get embedded because of ambiguous, inconsistent and incomplete requirements, leading to improper design and implementation, and the end result may be an unsafe system. The risk/hazard in the system may lead to catastrophic failures. Hence, an early prediction safety model must contain precise and complete requirements, which should be validated by the client who is the source of requirements and also should be explainable to all the other stakeholders. The stakeholders have different skill set, and hence, there should be a common language to model the system for early safety prediction.

4.3 Solution Strategies

In this section, two new approaches have been proposed to address the two folded research problems discussed above. The first proposed approach consider and tackles difficulty in generalization of the quantitative safety analysis method. The second

proposed approach deals with the uncertainty problem in State-space safety models. The proposed approaches are being discussed in Section 4.3.1 and 4.3.2 respectively.

4.3.1 Strategy for dealing with the difficulty in generalization of the quantitative safety analysis methodology

We propose, a new probabilistic approach to quantify safety of safety-critical system based on probabilistic safety assessment (PSA) to deal with the shortcomings of the existing techniques discussed in Section 4.2.1. The proposed methodology considers both hardware and software for the quantitative assessment of SCS. CBS is the complex system, in which components can be arranged in series, in parallel or in combination of both. This methodology works on all kind of CBS, irrespective of the arrangements of the components. The methodology has been tested on 29 operational data sets of Digital Feed Water Controller System (DFWCS) to validate its effectiveness. A real case study of DFWCS of a nuclear power plant is taken to show the effectiveness of this methodology.

4.3.2 Strategy for dealing with the uncertainty in State-space safety models

For the requirement of modeling the early safety prediction of a system, that should be explainable to all the stakeholders, an approach is proposed to support system safety engineering from requirements to deployment level, through proper analysis and suitable mappings. UML has already being proved as a general-propose modeling language in the field of system engineering that can be understood by all the stakeholders [139]. UML has an ability to model the scenarios of the system. In the paper [140], authors have extended the UML to incorporate dynamic aspects for Schedulability, Performance and Time Specification. Based on this, it is possible to extend the UML further to make it appropriate for safety modeling and safety quantification of a system. We propose a methodology to convert the UML model into the state space model that can be used to analyze the critical attributes of the systems and predict the system safety. The resultant safety model is a PN model, which is then extended to model the probabilistic occurrence of system failure. The proposed approach is validated on 13 sets of operational profile of Reactor Core Isolation Cooling System (RCICS) for different safety critical systems of Nuclear Power Plant.

4.4 Conclusion

In this chapter, research problems are formulated. These are: 1) an analytical approach to quantifying safety, relying on analytically solvable models that are hard to generalize, and 2) uncertainty in State-space models. The respective solution strategies to tackle those problems are also discussed.

In the Chapter 5 and Chapter 6, based on research problems, the respective proposed approaches are being discussed and illustrated with is proposed with a NPP as a case study. Chapter 5 is our second contributory chapter.