Chapter 7

Conclusion and Future Research

Traditionally, analytical approaches are used for reliability and safety modeling of a system. In this thesis work, we have discussed the limitations of two major critical dependability attributes namely Safety and Reliability. To address some of limitations, we have proposed frameworks that support System Reliability and Safety Engineering (SRSE) from requirements to deployment with adequate analysis through appropriate mappings.

One of the prime potential benefits of early safety prediction of a Safety Critical System (SCS) is to take preventive action for achieving the target safety level of a SCS. Therefore, researchers are continuously to proposing various approaches to predict the safety of an SCS during early phases of Safety Critical System Development Life Cycle (SCSDLC). Many of the existing models, during SCS design phase, are state space models, but the uncertainties associated with the accuracy of the model, parameters, phenomenon and assumptions limit their practical usage.

In this thesis work, two issues have been addressed: (i) Difficulty in generalizing the quantitative safety analysis methodology. (ii) Uncertainty in State-space models. The specific conclusions of proposed methodology to solve the above mentioned two issues are highlighted in the following sections.

7.1 Difficulty in Generalizing 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. We have proposed and introduces a framework to address the said generalization difficulties. Our framework contains six phases; each phase has been explained and demonstrated with the help of a case study. The idea is to model a system that starts with the development of a state machine from a logical perspective of a system and convert it into Markov model. Therefore, the transition probabilities in between the states of Markov Chain (MC) is computed and assigned based on SIL (IEC61508). A tool TimeNET is used for steady state analysis. This methodology is applied and demonstrated on the digital feed water controller system (DFWCS) of a nuclear power plant taken as a case study. The methodology has been tested on 29 operational profile data sets of DFWCS for 3 years to validate its effectiveness. The results indicate that the method can identify possible hazards

and quantify such hazards of a SCS. Brown and Lipow Input domain model which is suitable for real-time systems, is used for validation of the proposed approach.

7.2 Uncertainty in State space Models

There are different approaches available in the literature to predict the safety of a system using state space models. A good safety prediction model should consider and must include all the functional and non-functional requirements of the system. For accuracy of the model, concerning the requirement integrity is a principal objective. Hence, UML has been extended for the creation of such a model. The purpose of using UML is to construct a safety model with the involvement of all the stakeholders, especially the clients/end users. UML can capture all the requirements and be easily understood by all the stakeholders is the reason to choose it. The concepts used in our approach is to predict safety of a SCS from requirement specifications by extending it to a model are 1) the mapping of UML state chart as deterministic model for capturing requirements of a system into Petri Net (PN) as state space model for behavioral analysis of different states of a system, and (2) state transition probabilities derived from IEC 61508 based on SIL of different states of a system. The proposed methodology has been illustrated and validated on a SCS of an NPP. The detail description of the case study is described in section 6.3. The methodology is validated on 13 sets of operational profile data of Reactor

Core Isolation Cooling System (RCICS) for 3 year of different safety critical systems of NPP.

7.3 Future Work

In our approach of early prediction of safety for SCS using UML, we need to extend the model to include the time information, which is useful for real time systems, for performance analysis during the early phase. Some of limitations that are given in Chapter 3 and not covered in this thesis work are also subject to the future research. Further, for the usefulness of the state space safety model for different types of application, different parameters of the models need to be estimated. In the current trend of a software system development for SCS, many COTS are being used, which are black-box and difficult to expose its architecture. The future research may also include some methods to develop an architecture from the COTS test data to construct its safety model for safety assessment before actually deploying into the software system of a SCS. Further, our future work will investigate some critical issues for other important dependability attributes like reliability and security of SCS.