Chapter 1

Introduction

Present day critical systems are an aggregate of hardware-software with deadlines associated with tasks and more importantly safety-critical need to monitor safety norms violations. A safety-critical system executes the critical tasks, the failure of which may jeopardize human life, lead to considerable financial misfortune, or cause extensive environmental damage. The real challenges of software development are faced when we design a system that has to take care not only functionality but the monitoring of safety norms/conditions violations along with time critical completion of multiple tasks. Nowadays, safety-critical systems are being used in the military, nuclear power plants, medical care instruments, commercial aircraft, and defense equipment. Failure in any one of the systems of the said zone these zones can rapidly prompt human life being placed in risk, loss of instrument and so on. Therefore, safety-critical systems must have to be dependable to minimize failure and their hazardous consequences. The ability of such systems to run reliably and safely has

become a focal and widespread concern. Safety turns into a primal appraisal in such systems where human lives can, by some means be placed in danger, expecting to agree to safety necessities defined by industry norms, i.e. ANSI/ISA S84, IEC 61513, IEC 61496 (EN 61496), etc. The concerted effort towards safety analysis of the systems has played a major role in improving and verifying the safety of systems. *The safety of a system is the conditional probability* that the system has survived the period during an exposure time interval without an accident, provided that it was functioning without catastrophic failure at start-time [1], [2]. During the past two decades, there had been several severe accidents. We illustrate only some of the important catastrophic accidents below out of many severe accidents that had taken place due to the failure of 1) hardware; 2) software; 3) hardware and software both; to realize the essence of dependability of system. The summary of some accidents is shown in Table 1.1 [3]-[14]:

1. ***Flydubai 737-800, Russia[3]:***

   Flydubai flight was an international flight scheduled on 19th March 2016, crashed in the early morning, at 3:42 P.M., during a landing process at the airport of Rastov-on-Don in Russia. This mishap was causing severe loss regarding sixty-two deaths including seven crew members. The flight is managed by Boeing 737-800 aircraft, scheduled arrival from the international airport of Dubai, United Arab Emirates. When, flight reached the airport, that time Rastov-on-Don Airport was facing inclement weather. The first attempt

at the landing of the flight aborted and went to a holding sequence for the second attempt which took approximately two hours. After the failure of two landing attempts the flight climbed nearly 1.2 km height then started falling and near the runway crashed.

Investigators are examining various possible causes, including human error, a technical failure, and bad weather conditions. Earlier, Russian investigators were quoted as saying they believed a pilot error or a technical failure was the most likely reason for the crash. Most probably this mishap occurs due to failure of the weather forecast systems.

2. ***Fukushima nuclear disaster, Japan[4]:***

   On March 11th, 2011 an enormous earthquake and the next tsunami triggered the cooling down of the reactors and the cooling down of the put in fuel pools of the Fukushima Daiichi nuclear plant to fail. A non-stoppable nuclear catastrophe unveiled. The discharge of radioactive materials took place through pressure relief, uncontrolled release of radioactive heavy steam, fires, explosions, leakage and seepage of thousands of liters of polluted water. So far as the misfortune attained 2 were dead, 37 heavily injured, around 150,000 individuals were evacuated, and the full total damage was $13 billion in response to the mishap.

   Once the earthquake occurred, subdivision 1 of the Fukushima Daiichi plant was at normal functioning at the priory specified electricity output corresponding to its technical specifications; subdivision 2 and 3 were in operational

phase within the rated heat parameters with their specifications and subdivisions 4, 5 and 6 were going through periodical inspections. The tsunami triggered by the earthquake flooded and completely ruined the emergency diesel generators, the seawater cooling down pushes, the electric wiring system and the DC power for subdivisions 1, 2 and 4, leading to lack of all power except for an exterior supply to subdivision 6 from an air-cooled emergency diesel generator. In a nutshell, subdivisions 1, 2 and 4 lost all electric power; sub-division 3 lost all AC electric power, and later lost DC before the dawn of March 13, 2012. Sub-division 5 lost all AC electric power. The loss of electricity managed to get very hard to efficiently cool off the reactors on timely and caused the reason behind the explosion.

3. ***Crash of Air France Flight 447[5]:***

   On, MAY 31, 2009, an aeroplane Airbus A330-200 departed from the Rio de Janeiro-Gale˜ ao, Brazil Airport Terminal, to reach in Paris, 11 hours later, it crashed into the Atlantic Sea on June 1. The aeroplane was transporting 216 travelers, and 12 staff members, most of whom are presumed to be dead. As well as the loss of the aeroplane itself, Air France released that every victim's family would be paid approximately EUR17, 500 in preliminary compensation. This incident makes it be the deadliest catastrophe for Air France, surpassing the Air France flight 4590 in 2000 that wiped out 109 people.

   Regarding software related supporting factors, the onboard automating confirming system sent several text messages regarding discrepancies in

the indicated air velocity (IAV) readings before the aeroplane disappeared. Altogether, 24 error text messages were made as systems failed over the aeroplane. On June 4, 2009 (three days after the crash of aeroplane 447), Airbus released a primary Accident Information Telex to operators of most Airbus models reminding pilots of the advised Abnormal and Crisis Procedures to be studied regarding unreliable airspeed sign. Efforts to get the airline flight data recorders, critical to deciding the exact reason behind the crash, continued in Feb 2010, however, the chance of restoration was low. The final survey on the crash was released by the end of 2010.

4. ***Cedar Sinai Medical Centre in Los Angeles, California[6]:***

   A software misconfiguration in a CT scanning device used for brain perfusion scanning at Cedar Sinai INFIRMARY in LA, California, led to 206 patients acquiring radiation doses about 8 times greater than expected during an 18-month period starting in Feb 2008. Some patients reported momentary hair falling and erythema. The U.S. Food and Medication Association (FDA) has predicted that patients received dosages between 3 {Grey} (Gy) and 4 {Grey} (Gy).

Table 1.1: Catastrophic accidents in the last decade

Name of Accident	**Year**	**Level of Severity**	**Losses**	**Reason**
Flydubai 737-800, Russia	19/03/2016	Medium	62 Died	Maybe failure of weather forecast systems

Metrojet Flight 9268, Egypt	31/10/2015	High	224 Died	May possible causes of the crash included a fuel explosion, metal fatigue, and lithium batteries overheating
Indonesia AirAsia Flight 8501, Indonesia	28/12/2014	High	162 Died	Rudder travel limiter failure leading to inappropriate pilot response
Malaysian Airlines Flight 370, Malaysia	08/03/2014	High	227 Missing	Contact loss from the ground
Lac-Mégantic derailment, Canada	06/07/2013	High	47 Died	Nonresponsive system towards brake applied
Buenos Aires Rail Disaster,Argentina	22/02/2012	High	142 Died, 368 Injured	Failure of brake system
Railway signaling failure, Sydney	12/04/2011	Medium	40 percent of train delay	Failure of Software ATRICS to properly respond to the partially failed switch
Fukushima nuclear disaster, Japan	12/03/2011	High	37 Injured, Loss of $ 23.6 billion	Failure of emergency cooling caused an explosion
Crash of Air France Flight 447	31/05/2009	High	228 Died	On-board automotive report system transmitted 23 error messages
Cedar Sinai Medical Centre in Los Angeles, California	2008- 2009	High	206 patients, wrong dosages	Misconfiguration of software used by CT scanner for brain perfusion scanning
Emergency Shutdown of the Hatch Nuclear Power Plant	07/03/2008	High	Loss of $ 5 million	Software up gradation causes to the reset the data in I&C system
Hartsfield-Jackson Atlanta International Airport, USA	19/04/2006	Medium	Delay of 120 flights	False alarm due to malfunction of software

Loss of Communication between the FAA Air Traffic Control Center and Airplanes	14/09/2004	High	Disrupted about 600 flights (including 150 cancellations)	A bug in a Microsoft system compounded by human error
Loss of the Mars Polar Lander	03/12/1999	High	Loss of $ 120 million	One of the magnetic sensors attached to the landing legs tripped during descent resulting in a premature shutdown of the engines
Crash of Korean Air Flight 801	05/08/1997	High	228 died, 26 seriously injured	Failure of Minimum Safe Altitude Warning (MSAW) system

1.1 Need of Safety Analysis for Safety Critical Systems (SCSs)

Given the above ascribed accidents, today, safety has become a critical issue in the case of critical applications. The impact of failure varies from minor inconvenience and prices to personal injuries, major economic loss, and death. Reasons for failure comprise lousy engineering design, defective manufacturing, insufficient testing, human error, poor maintenance, improper use, and inadequate protection against excessive stress. A number of the other factors that also play an instrumental role in specifying the requirement for better safety are government regulations, public

pressures, and rising number of litigations. To minimize failures in engineering systems, it is essential to know why and how failures happen. It is also crucial to understand how frequently such failures may occur. Safety analysis evaluation ensures that the effects of failures are minimum. Thus, the safety evaluation process is an inherent part of the system development process.

The primary objectives of safety analysis approaches [15], [16], [17] are as follows:

1. To identify safety requirements and associated safety constraints.
2. To understand how a situation can be made safer.
3. To identify critical components.
4. The requirement of redundancy.
5. To improve the design process.
6. To schedule preventive maintenance programs.
7. Replacement and residual life estimations.
8. Safety management.
9. To assess the life cycle cost.

Today, numerous methods are available but no single method guarantees to fulfill all the objectives enumerated above.

1.2 History of Safety

The history of safety may be traced back to the Code of Hammurabi (2000 B.C.) considering the article "A Short History of System Safety" that states "if a house falls on its occupants and kills them, then the builder shall be put to death" [18]. In the modern times, a patent was given for first impediment safeguard in the United States of America in 1868 [19]. In 1893, U.S. Congress passed the Railway Safety Act, and in 1912, assembly was held by the cooperative Safety Congress in Milwaukee, Illinois [19], [20]. In 1931, the very first book "Industrial Accident Prevention" was released [21]. In 1947, a paper entitled "Engineering for Safety" was introduced to the Institute of Aeronautical Sciences [22]. It highlighted the importance of design safety into aeroplanes. In 1962, the U.S. Airforce launched Display 62-41 entitled "System Safety Engineering for the Development of Airforce Ballistic Missiles." In July of 1969, MIL-STD-882 was released; it was titled, "System Safety Program for Systems and Associated Subsystems and Equipment: Requirements for." This milestone focuses on enlarging the range of system safety that might apply to all military services in the Department of Defense (DoD). The entire life cycle method of system safety was also introduced during this time. In 1970, the United States Congress passed the occupational safety and health act (OSHA). In June 1977, MIL-STD-882A was introduced in which the significant contribution was based on the idea of risk acceptance as a criterion for system safety. This evolution needed an introduction of risk probability and recognized categories for frequency of occurrence to adapt the long standing. In March of 1984, MIL-STD 882B was

released. It included an important reorganization of the !/ A !/ version. Again, the development of in-depth guidance in both engineering and management requirement was obvious. The task of sorting through these demands was becoming complicated, and much more conversation on tailoring and risk approval was expanded. In January 1993, MIL-STD-882C was released. Its important change was to combine the hardware and software system safety efforts. In the mid 90's, the DoD acquisition reform motion started, together with the Military Specifications and Standards Reform (MSSR) initiative. Both of these movements resulted in the development of a standard pattern for system safety in MIL-STD-882D, introduced in February of 2000 [18]. Through the years, several organizations, scientists, and writers have led to the development of the safety analysis field.

1.3 Motivation and Objectives of Research

After realizing the substantial benefits of early quantification of Computer Based System (CBS), several recent approaches have begun an assessment of safety regarding high-level system structure. These approaches model safety-critical systems, some of them are based on state space model. A model should include all the functional and non-functional requirements. Generally, a CBS may fail because of ambiguous or incomplete requirements or due to defect in system design. Ambiguous requirements also penetrate defect in the design. Therefore, a safety assessment model must contain precise requirements. All of the existing

methodologies have taken are 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. This issue has been more elaborated and addressed in this thesis work in Section 4.2.1 of Chapter 4.

Some existing state-space modeling techniques discussed in the Section 4.2.2 are useful to model the system for analyzing its critical quality attributes like reliability and safety for which it is necessary to embed all the requirements in the model. However, it is a challenge to build a model which covers all the requirements and dynamic aspects of system behavior. Construction of state space model has two known issues: 1) validation of consideration of all the system requirements; 2) requires expertise and hence not easily understood by all the stakeholders, especially the clients, who may not be aware of modeling techniques. Hence, clients who are the prime source of requirements cannot know whether the constructed system safety model has taken care of all the requirements. These issues have been more elaborated and addressed in Section 4.2.2 of Chapter 4. The following objectives of this thesis work will be addressed in the forthcoming Chapter.

1. To identify the major design weaknesses.

2. To find out the system feasibility.

3. To provide models for system dependability analysis.

4. To establish the goal for behavior tests.

5. To improve decision-related to business such as budget allocation and scheduling.

1.4 Scope of Research

1. The proposed methodologies in this thesis work are applicable to any kind of Safety-critical system and the case studies have been focused only on safety systems of Nuclear Power Plant (NPP).

2. All the proposed models are available in the form of analytical expression for the quantification of associated parameters.

3. In the case of embedded software systems, the wear and tear-out of the chip in which software resides have not been considered.

1.5 Thesis Outline

The organization of the thesis is organized as follows:

Chapter 2

This chapter provides background related to safety which needs to understand the reasoning presented further throughout this thesis. It starts with a brief overview of dependability showing safety as one of the attributes. The main focus is given on

the studies of various state space modeling techniques used for early prediction of dependability attributes of a system.

Chapter 3

In this chapter, a comprehensive review of literature for early prediction of system reliability and safety are present in the context of the research objectives defined in Chapter 1. Further, the Chapter also illustrates limitations, that the existing analysis techniques have, and same is shown in the form of following groups: 1) *Modeling limitations:* Usually modeling limitations are because of the assumptions we make to ensure model expansibility, which may lead to unsafe estimation, 2)*Analysis limitations:* Analysis limitations are due to lack of analysis techniques, 3) *Parameter estimation limitations:* parameter Estimation limitations are because of non-consideration of different system artifacts, 4) *Validation limitations:* Validation limitations are because of paying little effort to validate the estimated dependability attributes and 5) *Optimization limitations:* Optimization limitations are because of non-consideration of complex interactions among components in the architectural design.

Chapter 4

In this chapter, the formulation of the research problem, based on the extensive literature review and various planned solution strategies for the identified problems, is presented. The limitations of existing approaches are brought out in the previous

chapter, Chapter 3. The uncertainties along with their treatment for early prediction of system safety are discussed. The solution strategies for the stated limitations regarding the early prediction of system safety are also discussed in Chapter 3. Further, the Chapter also proposes and illustrates a procedure to computes the safety estimates during Safety Critical System Development Life Cycle (SCSDLC).

Chapter 5

In this chapter, a framework for quantitative probabilistic hazard assessment of a safety critical and control system, with a case study of the control system of an NPP is proposed. Some related works are also discussed in this chapter, from that we conclude that in the existing approaches, the authors have assumed methodologies that have been based on some coarse knowledge or have been computed using analytical methods that do not give accurate values. Some authors have quantified hazards using an operational profile, but that is possible only after deployment of the system, and hence, it is not an early prediction. The proposed framework is useful in overcoming the limitations of the existing methods, and the validity of this approach has been proven by 29 operational data sets of SCS. The application of our framework has been shown step by step on the Digital Feed Water Control System (DFWCS) of a pressurized water reactor (PWR) of an NPP. The work in this chapter concentrates on improving the current methodology to assess the safety-related hazards of a safety-critical system. Also, this can apply to all types of systems that can be designed or modeled.

Chapter 6

UML has extensively being used for modeling system in the literature, and hence it can be a good idea to obtain a state space model from corresponding UML model for being able to analysis both the structural and behavioral proposition of the concerned system. In this chapter, we propose a methodology with respect to structural and behavioral properties for a purpose that can be used to verify. State-space models have a potential to verify the system with respect to its structural and behavioral properties. However, there is no standard mechanism to create state space models of the systems, directly from the functional requirements. UML is a modeling language that can be well understood by all the stakeholders and hence it is easy to do UML modeling. In the present Chapter, we proposed a framework for safety analysis in terms of quantitative probabilistic hazard assessment by using tranformation of UML state-chart diagrams into Petri Nets for system analysis of the SCS. The failure rates used in this approach are based on SIL (IEC 61508). The approach has been validated on 13 sets of operational profile of different safety critical systems of NPP and in this Chapter; it is demonstrated on Reactor Core Isolation Cooling System (RCICS) of an NPP. The result of the proposed approach shows its effectiveness.

Chapter 7

The final conclusive remarks, observations, and understandings obtained throughout the thesis are summarized in Chapter 7 as conclusions. The chapter makes out

possible indication for the future work as well.