Annals of Nuclear Energy 105 (2017) 133–143

Contents lists available at ScienceDirect

Annals of Nuclear Energy

journal homepage: www.elsevier.com/locate/anucene

Transformation of deterministic models into state space models for safety analysis of safety critical systems: A case study of NPP

Vinay Kumar *, Lalit Kumar Singh, Anil Kumar Tripathi

Dept of Comp. Sc. & Engg, IIT (BHU), Varanasi, India

ARTICLE INFO

Article history:
Received 11 July 2016
Received in revised form 17 January 2017
Accepted 25 February 2017

Keywords:
Petri Nets
State-chart diagram
State space modeling technique
UML

ABSTRACT

The state space models has been successfully applied in engineering, statistics, computer science and economics to solve a broad range of dynamical systems problems; like safety analysis, reliability analysis, performability analysis, etc. However, embedding the complete and accurate system requirements in such models is quite challenging. Analyzing model with incomplete or inaccurate requirements gives inaccurate results. UML is a proven and easy approach to capture all the system requirements. This paper proposes a methodology to transform the UML model into the state space model. The resultant model will embed all the system requirements and hence can be used to analyze the critical attributes of the systems. The methodology is validated on 13 sets of operational profile of different safety critical systems of Nuclear Power Plant and shown on Reactor Core Isolation Cooling System (RCICS).

1. Introduction

Dynamical analysis of the system is used to describe the behavior of complex systems and hence is useful for verification and validation. Validation ensures the conformance of functional and non-functional requirements. Non-functional requirements are often expensive but add quality. Non functional requirements are constraints on the system design. They may arise from user requirements, technical disciplines or the external environment. They are often "ilities", can be divided into product or support constraints and include reliability, safety, security, etc. Therefore, safety critical systems need to be validated with respect to the non-functional requirements.

State space models are widely used to analyze non-functional requirements. However, these models are not easily understood by all stakeholders and creation of these models requires technical expertise. UML is easy to understand for all stakeholders and has a potential to capture all the requirements. But it is not capable to perform dynamical analysis for which state-space models are required. In this paper, we attempt to transform the UML model into a state space model, Petri Nets for the system dynamical analysis. Petri Net (Murata, 1989) is a graphical and mathematical tool and widely used for dynamical analysis of the systems. We validate the approach on a NPP system, known as RCICS.

The remainder of this paper is as follows: In Section 2 we give the literature survey of the methodologies for dynamical analysis of the systems along with their shortcomings. A complete case study of RCICS along with its model is given in Section 3. Section 4 describes our approach to transform UML state-chart diagrams into Petri Nets for dynamical analysis. Also, in this section, we demonstrate and validate our approach on the case study. Section 5 concludes this paper.

2. Preliminaries and related work

This section is divided into two parts: (1) brief introduction of UML and Petri Net used are discussed and (2) close related work in this area.

2.1. Preliminaries

2.1.1. Unified modeling language (UML)

UML is the most interesting and a valuable tool in the area of system development. The UML is a visual modeling language that allows system developer to develop blueprints that capture their versions in a standard, simple-to-realize way, and offers a

Abbreviations: RV, Re-circulation Valve; RCICS, Reactor Core Isolation Cooling System; RP, Re-circulation Pump; RCICT, Reactor Core Isolation Colling System Turbine; RCICP, Reactor Core Isolation Colling Pump; CST, Condensate Storage Tank; SP, suppression pool; NPP, Nuclear Power Plant; PN, Petri Net; SRV, Safety Relief Valve; USCD, UML State Chart Diagram.

* Corresponding author.

E-mail addresses: vinay.rs.cse13@iitbhu.ac.in (V. Kumar), lalit.rs.cse@iitbhu.ac.in (L.K. Singh), aktripathi.cse@iitbhu.ac.in (A.K. Tripathi).

http://dx.doi.org/10.1016/j.anucene.2017.02.026
0306-4549/

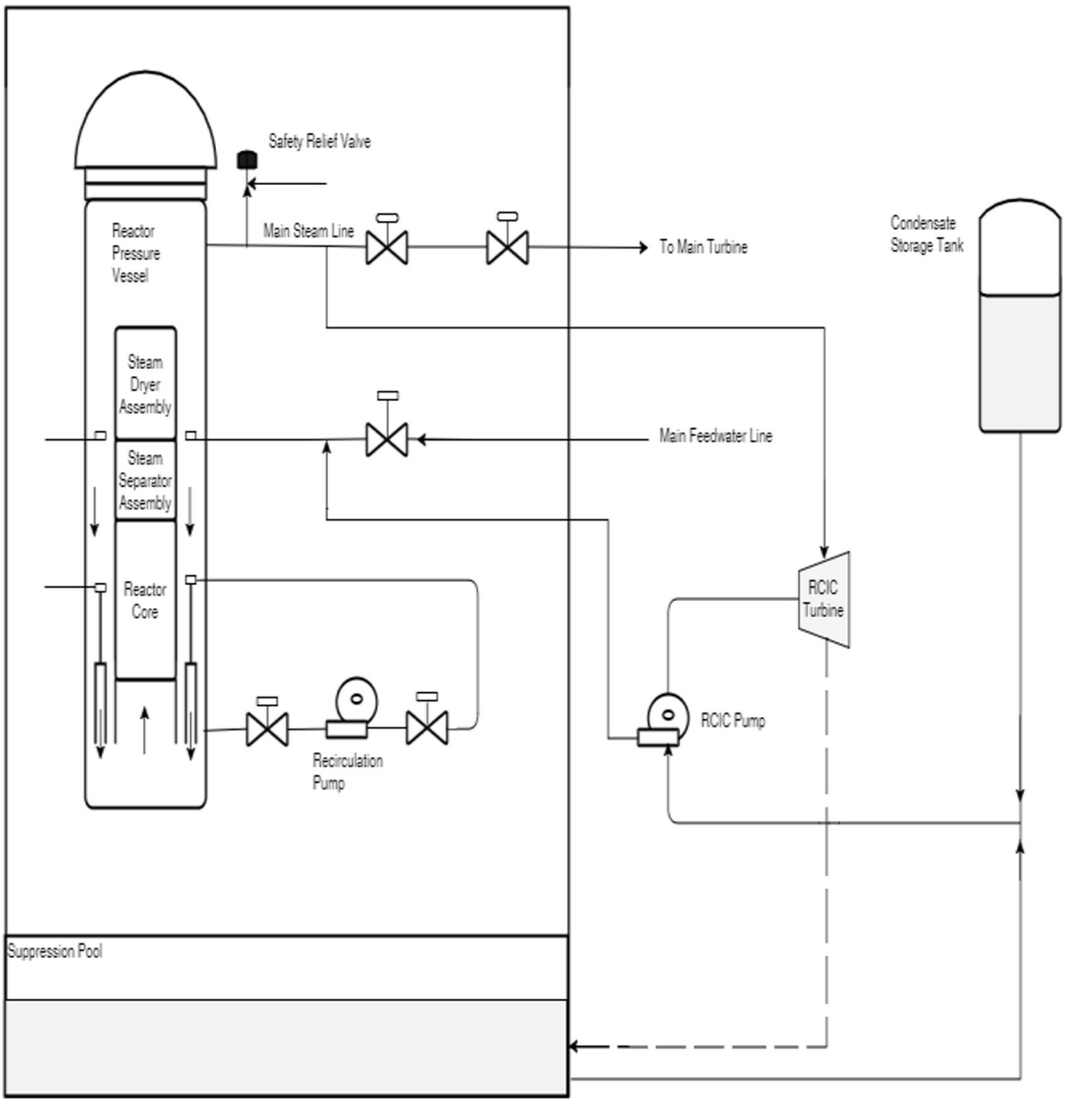

Fig. 1. The RCICS outlay.

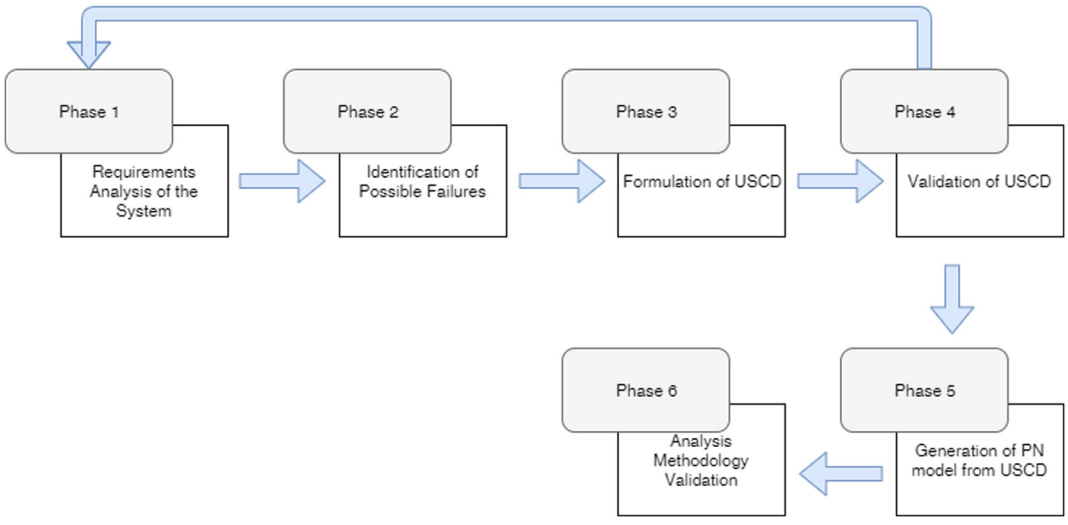

Fig. 2. UML to PN mapping framework.