Reliability Engineering and System Safety 149 (2016) 1–13

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Stochastic hybrid automaton model of a multi-state system with aging: Reliability assessment and design consequences

F. Chiacchio [a,*], D. D'Urso [a], G. Manno [b], L. Compagno [a]

[a] Dipartimento di Ingegneria Industriale, Università degli Studi di Catania, Italy
[b] DNV GL, Strategic Research & Innovation, Høvik, Norway

ARTICLE INFO

Article history:
Received 2 July 2015
Received in revised form
8 December 2015
Accepted 12 December 2015
Available online 23 December 2015

Keywords:
Dynamic reliability
Stochastic Hybrid Automaton
Simulink Reliability Modelling
Monte Carlo simulation
Hybrid Basic Events

ABSTRACT

Dynamic reliability aims to relax the rigid hypotheses of traditional reliability enabling the possibility to model multi-state systems and consider changes of the nominal design condition of a system. The solution of such type of models is a complex task that cannot be tackled with analytical techniques and must involve other types of formalisms based on simulation. One of the most promising simulation approach is Stochastic Hybrid Automaton (SHA), able to breakdown a system into a physical and a stochastic model that are coupled together with shared variables and synchronising mechanisms.

In order to foster this latter research path, a simulation model, based on SHA, was codified as regard to a case of study; it has allowed to compute the reliability of a multi-state aging system under dynamic environmental and operational conditions. The same model has permitted to understand the system behaviour resulting a useful tool for its design. Such type of highlights could not be inferred using traditional reliability modelling, as shown in the comparison with a dynamic fault tree.

The SHA model was codified in Simulink environment and represents a small step ahead for the conception and the delivering of a user-friendly tool for the DPRA.

1. Introduction

Traditional techniques of reliability assessment have been developed under hypotheses that simplify many real-life boundary conditions. This is probably the price paid in the early 30's when the reliability theory started to gain importance and, under the pressure of new technological advances in the military, maritime, Oil & Gas and aircraft industries, grew fast and rigid. Such industrial applications can never stop, work under well defined conditions and perform within narrow operating margins for the entire time of the mission. For these applications, the actual definition of reliability has offered a well-defined theoretical domain, such that the mathematics built-up around resulted elegant and robust [1]. From a practical point of view, such theory was applicable supported by the famous stratagem in engineering: think always the worst scenario.

Nowadays, the improvement of this conservative approach has brought to the conception of a new research field that encompasses many different subjects and goes under the name of performability [2].

Dependability is one of the attribute of performability; it represents an extension of reliability and deals with reliability, availability, safety and related measures of interest for a system [3,4]. In turn, dependability assessment considers also non-functional aspects related with the functioning of a system like reconfiguration, fault tolerance, interferences or dependencies and, more generally, its dynamic evolution. These elements allow overcoming the binary nature (i.e., fault or working) when modelling the operating state of a component and relax the hypotheses of traditional reliability theory (i.e., statistical independence), giving room to more insightful analyses including performance evaluation in degraded conditions and considering the system evolution under different environmental and operational conditions. Actually, a complex system works under a multitude of different conditions whose sequence and durations can be stochastic or deterministic, therefore its operating rules and performance can change dramatically.

The need for more realistic reliability assessments started within the field of nuclear engineering, with the definition of the Dynamic Probabilistic Risk Assessment (DPRA) [5]. This class of problems, known also as Hybrid Stochastic systems [6] are characterized by the coupling of a physical deterministic model (i.e., first principles models) with a stochastic one. In this assembly, a stochastic event can trigger a change in the deterministic model and, mutually, a variation of the deterministic model modifies the

* Corresponding author.
E-mail address: chiacchio@dmi.unict.it (F. Chiacchio).

http://dx.doi.org/10.1016/j.ress.2015.12.007
0951-8320/

Acronyms

BDMP : Boolean Driven Markov Process
CTMC : Continuous Time Markov Chain
(D)FT : (Dynamic) Fault Tree
DPRA : Dynamic Probabilistic Risk Assessment
FSPN : Fluid Stochastic Petri Net
GSMP : Generalised Semi-Markov Process
HBE : Hybrid Basic Event
NHPP : Non-Homogenous Poisson Process
ODEs : Ordinary Differential Equations
PDAEs : Partial Differential Algebraic Equations
pdf : Probability Density Function
PDMP : Piecewise Deterministic Markov Process
RBD : Reliability Block Diagram
RSM : Regime Switching Modelling
SAN : Stochastic Activity Network
SEFT : State/Event Fault Trees
SHA : Stochastic Hybrid Automaton
SHA-HPM : SHA-Hybrid Pair Model
SPDEs : Stochastic Partial Differential Equations

Others

ATU : Air treatment unit
EU : External unit
IU : Internal unit
T_f : Failure temperature [°C]
T_{co} : Control temperature [°C]
T_D : P_{cool} degradation threshold [°C]
T_i : Internal temperature [°C]
T_e : External Temperature [°C]
t_f : Failure exposure interval [h]
t_{exp} : Hours of exposure [h]
P_{cool} : Cooling power [W]
P_o : Data Cluster heating power [W]
R_{DC} : Reliability of the Data Cluster
R_{CS} : Reliability of the air conditioning system

operational conditions and the probability functions of the stochastic one.

In the literature, DPRA is also referred as Probabilistic Dynamics or Dynamic Reliability [7–10]; the term dynamic is used to address changes in the environmental and operational conditions. Another main difference with traditional quantitative techniques [2] like Static Fault Trees (SFT) and Reliability Block Diagrams (RBD) is the possibility to model more accurately the aging effects in a system. As matter of fact, in a DPRA a component degrades only during the intervals of time in which it is operating, as opposed to conventional analyses where aging factors are usually given as inputs to the analysis.

At the state of the art, there are analytical and simulation techniques that can be used to handle a DPRA problem. Among the former, Piecewise Deterministic Markov Process (PDMP) [10–12] and Regime Switching Modelling (RSM) [13,14] are solid mathematical frameworks able to model both aging effects and system evolution. PDMP models the aging evolution of a system with a set of differential equations while RSM the dynamic change of the system with a sequence of Continuous-Time Markov Chains (CTMC), each one describing a particular type of environmental/operational condition. An alternating renewal process governs the regime switching from a CTMC to another. Also state space modelling has been recently applied to dynamic reliability with aging; [9] offers an elegant review of the most suitable analytical methods, including Generalised Stochastic Markov Processes (GSMP), able to address several dynamic reliability behaviours such as, fault coverage, load sharing, fault coverage. Moreover, it provides a useful guideline flowchart that shows what modelling approach is best to use with respect to the problem to undertake.

With the increasing of computing power, simulations can result a valid alternative and may in fact be the most suitable approach for complex DPRA models. In particular, simulations allow the analysis of systems with non-Markovian structure, as shown in [15], for an application in the Oil & Gas sector. Simulation can be implemented with plenty of different tools, from a spreadsheet [16] to other well-known high-level tools, like Simulink [17] and can benefit of several speed up algorithms [18,19]. Other research contributes show how hybrid stochastic models like Fluid Stochastic Petri nets (FSPN) [20] and Stochastic Activity Networks (SAN) [21,22] can be used to implement a continuous process with stochastic features and simulate dynamic reliability problems. In fact, besides the elements of traditional Petri Nets, hybrid stochastic models present additional objects that allow the characterisation of a continuous/discrete marking and time-dependent activities. Such models are then solved using a discrete event simulation engine. Although the penetration of these modelling formalisms within the industrial fields is nowadays a fact, it must be pointed out that the flat representation of a complex Petri Net, made up of places and activities, can become large and difficult to interpret, even more when describing a continuous process typical of a mechanical or a physical system. Hierarchy is a feature that has been often used to alleviate this issue; for instance, SHARPE [23] can combine SFT, GSPN and Markov Chains, RAATSS [24] supports DFT and ATS while MÖBIUS [25,26] offers high-level constructs (JOIN and REP) to build up composed hierarchical SAN models based on simpler atomic models which can be developed independently, replicated and joined. In particular, the construct REP allows to replicate an atomic model, while the construct JOIN permits the combination of two or more atomics on the base of a set of shared variables.

These hybrid formalisms are very powerful and general but do not offer any high-level construct for modelling systems characterized by physical and mechanical interactions. In these cases, the main drawbacks is the effort linked with the maintenance and the handover of such models. For these reasons, authors recognise the importance to make further investigation on promising hybrid modelling like Stochastic Hybrid Automaton (SHA), for the resolution of DPRA as the one shown in [6,27–29] and the utilisation of other tools, more indicated to describe dynamic systems. Among the several attributes of dependability this work deals with the reliability assessment under a dynamic reliability point of view.

Therefore, starting from the definition of system reliability, the DPRA modelling is gradually introduced with the inclusion of the aging effects and of the dynamic changes of the working/operative conditions of a system.

This first section clarifies why analytical techniques, like PDMP, GSMP or RSM, fail the resolution of such models. Afterwards, a non-trivial case study for the reliability assessment, possessing all the characteristics of a DPRA problem will be presented to better show the dynamic multi-state nature of a DPRA model.

The attempt to use a RAMS technique model like DFT, BDMP or DBRD for solving the case study will confirm the limits of this reliability technique and highlights the need for a more powerful