Annals of Nuclear Energy 120 (2018) 127–154

Contents lists available at ScienceDirect

Annals of Nuclear Energy

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

Dependability analysis of safety critical systems: Issues and challenges

Raj kamal Kaur [a,*], Babita Pandey [a], Lalit Kumar Singh [b]

[a] Department of Computer Science & Engineering and Computer Application respectively, University of Lovely Professional, Phagwara, Punjab, India
[b] Department of Computer Science & Engineering, IIT (BHU), Varanasi, India

ARTICLE INFO

Article history:
Received 20 July 2017
Received in revised form 20 April 2018
Accepted 13 May 2018

Keywords:
Safety-critical system
Dependability
Metrics
Dependability analysis techniques

ABSTRACT

Safety critical systems progressively used in domains such as nuclear power, transport, medical and information systems are often concerned with a formal process of dependability certification. The intent of dependability process is to ensure that these systems will deliver the expected services to its users. In order to ensure the dependability of large safety-critical systems, the software engineer or security professional needs a thorough knowledge of the process of dependability analysis. In the past several decades, a significant amount of attention has been devoted to the dependability assessment of safety-critical control systems from some perspectives such as reliability, availability, safety, and security. However, for analysis of the critical systems, there is no any universal accepted rigorous dependability analysis process, which helps to choose the metrics, techniques and methodologies for the dependability evaluation of such critical systems. This paper provides a comprehensive detailed literature survey in order to investigate different metrics, threats, means, techniques and methodologies to ensure the dependability of computer-based critical systems. The limitations of these elements are also analyzed with respect to their applicability in SC systems. In addition to this, highlighted various issues (gap), challenges and needs in the context of such systems. The direction for future research is suggested to extend the future scope of research. The purpose of this paper is to interpret a rigorous review concept, of relevance across a wide range of affairs. Therefore, this work helps to the academicians, researchers, and practitioners to put this into practice, analyze the shortcomings of existing research and identifying the open areas that are important for the related community.

Contents

1. Introduction . . . 128
2. Literature review . . . 130
 2.1. Limitation of the existing work . . . 130
  2.1.1. State space explosion . . . 130
  2.1.2. Missing metrics. . . . 130
  2.1.3. Static nature . . . 137
  2.1.4. Mitigation of the identified issues. . . . 137
  2.1.5. Simple case studies . . . 137
  2.1.6. Late software level (testing). . . . 137
  2.1.7. Security . . . 137
  2.1.8. Components-based analysis: . . . 137
  2.1.9. Simple Petri Nets:. . . . 137
  2.1.10. Transformation: . . . 137
3. Methodology. . . . 138
 3.1. Research questions . . . 138
 3.2. Search strategy . . . 138
 3.3. Inclusion criteria . . . 138

* Corresponding author.
E-mail address: grewal.rajkamal03@gmail.com (R.k. Kaur).

https://doi.org/10.1016/j.anucene.2018.05.027
0306-4549/

Nomenclature

SCS	Safety-critical system
MTBF	Mean time between failures
MTTF	Mean time to failure
MTTR	Mean time to repair
FTA	Fault tree analysis
FMEA	Failure modes and effect analysis
RBD	Reliability block diagram
ETA	Event tree analysis
AT	Attack tree
RAG	Resource allocation graph
CC	Cyclomatic complexity
PN	Petri net
DTMC	Discrete Time Markov Chain
SLR	Systematic Literature Review
COTS	Commercial off-the-shelf
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
NIST	National Institute of Standards and Technology
ISA	International Society of Automation

The singular & plural of an acronym are always spelled the same.

4. Dependability prediction metrics of SCS/(RQ1) . . . 139
   4.1. Primary attributes of dependability . . . 139
      4.1.1. Reliability . . . 139
      4.1.2. Availability . . . 139
      4.1.3. Safety . . . 139
      4.1.4. Security . . . 141
      4.1.5. Maintainability . . . 141
      4.1.6. Performability . . . 141
   4.2. Secondary attributes of dependability . . . 141
      4.2.1. Robustness: . . . 141
      4.2.2. Accountability: . . . 141
      4.2.3. Authenticity: . . . 141
      4.2.4. Non-repudiation: . . . 141
5. Dependability threats and means (RQ2) . . . 142
   5.1. Threats . . . 142
   5.2. Means . . . 142
      5.2.1. Fault prevention . . . 142
      5.2.2. Fault tolerance . . . 142
      5.2.3. Fault removal . . . 142
      5.2.4. Fault forecasting . . . 143
6. Dependability analysis techniques of safety critical systems/ (RQ3) . . . 143
   6.1. Analytical verification . . . 144
      6.1.1. Overview, Scope, and complement of analytical verification modeling techniques . . . 144
      6.1.2. Comparisons of analytical techniques . . . 147
   6.2. Experimental assessment techniques . . . 149
7. Result and discussion/ what is the observation of the existing research? (RQ4) . . . 151
   7.1. What is the observation of the existing research? . . . 151
   7.2. What is the gap in existing work and provide the idea for the new research? . . . 151
   7.3. Importance of security in dependability analysis . . . 151
   7.4. Challenges (what are the open issues that need to be resolved?) . . . 152
   7.5. Research priorities . . . 152
8. Conclusion and future work . . . 152
   References . . . 153

1. Introduction

In the current scenario, consistent utilization of digital technology has been observed in all sectors of industries and society. Due to this, different kind of digital technology (such as software in heart pacemakers, anti-lock braking systems in vehicles, flight and routing control system in the transportation) has been deployed for the satisfaction of human needs.

This intelligent technology is usually intended to open up new possibilities such as permit us to work quicker, make life easier, provides safety, effectual automatic management of the rapidly developing state of affairs, and performance as well as monetary benefits (Littlewood et al., 1998). If this intelligent technology brings new services and efficiency; at the same time, they might compromise the system dependability. The failure of such systems can be catastrophic, causing harm to both human life and the environment. For instance, transport accidents, emergency shutdown of Hatch Nuclear Power Plant (NPP) and failure of the medical devices due to the software failure will cause monetary as well as the human loss (Avizienis et al., 2004). Dependability concept defined as (Avizienis et al., 2004) "the ability of the system to deliver services that can justifiably be trusted". Although dependability is synonymous to reliability, but the dependability is a global concept which evaluate from the attributes of reliability, availability, safety, security, performability, and maintainability, etc. In the dependability concept, it is essential that software that is widely used is dependable, which means that the software is available whenever needed and it operates in safe manner and reliable