Expert Systems with Applications 41 (2014) 5669–5679

Contents lists available at ScienceDirect

Expert Systems with Applications

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

A verification framework with application to a propulsion system

Bin Zhang [a,*], Marcos Orchard [b,c], Bhaskar Saha [d], Abhinav Saxena [e], Young Jin Lee [f], George Vachtsevanos [f]

[a] Department of Electrical Engineering, University of South Carolina, Columbia, SC 29208, USA
[b] Department of Electrical Engineering, Universidad de Chile, Santiago 8370451, Chile
[c] Advanced Mining Technology Center of the Universidad de Chile, Santiago 8370451, Chile
[d] Palo Alto Research Center, 3333 Coyote Hill Rd, Palo Alto, CA 94304, USA
[e] Stinger Ghaffarian Technologies Inc., NASA Ames Research Center, CA 94035, USA
[f] School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332, USA

ARTICLE INFO

Keywords:
Verification
Offline verification
Runtime verification
Monte Carlo simulations
Propulsion systems
Automated contingency management (ACM)

ABSTRACT

This paper introduces a novel verification framework for Prognostics and Health Management (PHM) systems. Critical aircraft, spacecraft and industrial systems are required to perform robustly, reliably and safely. They must integrate hardware and software tools intended to detect and identify incipient failures and predict the remaining useful life (RUL) of failing components. Furthermore, it is desirable that non-catastrophic faults be accommodated, that is fault tolerant or contingency management algorithms be developed that will safeguard the operational integrity of such assets for the duration of the emergency. It is imperative, therefore, that models and algorithms designed to achieve these objectives be verified before they are validated and implemented on-board an aircraft. This paper develops a verification approach that builds upon concepts from system analysis, specification definition, system modeling, and Monte Carlo simulations. The approach is implemented in a hierarchical structure at various levels from component to system safety. Salient features of the proposed methodology are illustrated through its application to a spacecraft propulsion system.

© 2014 Elsevier Ltd. All rights reserved.

1. Introduction

The modern systems have continuously growing demands for improving the safety and survivability when unexpected faults/failures occur, which may lead to critical damage, expensive downtime, costly repairs, and even loss of assets and lives. For instance, aircraft/spacecraft and other military and industrial assets are increasingly required to operate with improved reliability and autonomy; they must be designed, operated, and maintained in ways that maximize their performance and availability with the presence of faults while reducing costs. To meet these demands, many condition-based maintenance (CBM) and Prognostic and Health Management (PHM) strategies have been developed (Chen et al., 2012; Liu & Han, 2014; Orchard, Hevia-Koch, Zhang, & Tang, 2013; Tran, AlThobiani, & Ball, 2014; Zhang et al., 2011). The successful implementation of CBM and PHM requires the subsystems, such as modeling, fault detection and identification, failure prognosis, etc., are well-designed to meet the performance specification from designers and customers. For this reason, verification and validation (V&V) has become an essential and integral component of the design cycle and brought potential benefits including the reduction of the design timeline, reduction of the life-cycle costs, and the improvement of the performance and reliability (Roychoudhury, Saxena, Celaya, & Goebel, 2013; Zhang, Tang, DeCastro, & Kai, 2010).

Verification and validation (V&V) of complex systems has drawn considerable attention from academia and industries in various application domains and has met with limited success over the recent past (Bartak & Rovensky, 2014; Bertolini, Oliveira, Justino, & Sabourin, 2013; Cpalka & Zalasiński, 2014; Kumar, Hanmandlu, & Gupta, 2013; Luque-Baena, Elizondo, Lopez-Rubio, Palomo, & Watson, 2013; Ouchania & Mohamedb, 2014; Souri & Jafari, 2014; Villalobos-Castaldi & Suaste-Gómez, 2013). Simulation platforms, field testing and formal methods have been exploited as potential means to address V&V issues (Li, Li, Xu, Rizy, & Kueck, 2010; Ouchania & Mohamedb, 2014; Seidel, Donath, & Haufe, 2012; Souri & Jafari, 2014). The complexity of large-scale dynamic systems has presented major challenges to the V&V designer necessitating new engineering-based methods to assist in the conduct of V&V studies. Researchers and practitioners do not quite agree on basic definitions on techniques to arrive

* Corresponding author.
E-mail addresses: zhangbin@cec.sc.edu (B. Zhang), morchard@ing.uchile.cl (M. Orchard), bhaskar.saha@parc.com (B. Saha), abhinav.saxena@nasa.gov (A. Saxena), gjv@ece.gatech.edu (G. Vachtsevanos).

http://dx.doi.org/10.1016/j.eswa.2014.03.017
0957-4174/© 2014 Elsevier Ltd. All rights reserved.

at solutions. The consensus currently within the defense community and other research establishments regarding the definitions for V&V is as follows (Tang, Orchard, Goebel, & Vachtsevanos, 2011 and Vachtsevanos et al., 2006):

Verification: The process of determining that a model/system implementation and its associated data accurately represent the developer's conceptual descriptions and specifications.

Validation: The process of determining the degree to which a model/system and its associated data provide an accurate representation of the real world from the perspective of the intended use of the model/system.

Verification answers the question: "Have I built the system right?" (i.e., does the system as built meet the performance specifications as stated?). Validation answers the question: "Have I built the right system?" (i.e., is the system model close enough to the physical system and are the performance specifications and system constraints correct? (Vachtsevanos et al., 2006; Zhang et al., 2011). Different from verification, which usually depends on conceptual design and development, validation often relies on statistically sufficient data from system. System verification and validation activities are in support of system development activities to achieve system accreditation. Successful system accreditation occurs when an affirmative answer is obtained to the question: "Do I trust that the system will meet the system performance specifications within stated system constraints?"

This paper focuses on the topic of verification and introduces a generic framework with specific emphasis on model-based verification of a PHM system module. Different from the existing approaches (Ouchania & Mohamedb, 2014; Roychoudhury et al., 2013; Seidel et al., 2012; Souri & Jafari, 2014; Zhang et al., 2010), the proposed verification approach has novelties in the following aspects: (1) It is based upon the integration of system analysis, specification definition, modeling, and Monte Carlo simulations; (2) It extends traditional off-line verification into a combination with runtime verification; (3) It is featured with a hierarchical structure with verification at different levels. Due to these new features, the verification framework proposed in this paper requires more modeling and computing efforts. In addition, since this is a model-based verification, system modeling has direct impacts on the verification.

System model plays an important role in simulation-based off-line verification studies (Lee, Ryu, Lee, Shin, & Kim, 2010; Souri & Jafari, 2014; Vachtsevanos et al., 2006; Wei, Cai, Wang, Wang, & Gou, 2009). To better understand the system architecture, our approach decomposes a large-scale system into constituent constructs but also to capture their interactions. Structural and functional system models are developed towards that end. Then a generic verification architecture, consisting of off-line verification and runtime verification, is introduced to address major complexity issues. The verification of the complex system in the proposed approach is conducted at component-, system-, mission-, and safety-levels to guarantee the performance specifications are met for the system and the deployed PHM algorithms. The enabling technologies include mathematical tools for safety and optimization, temporal logic of actions, modeling and model check, and performance metrics. The developed verification approach is case studied on the automatic contingency management of a monopropellant propulsion system to demonstrate its efficiency for complex system verification.

2. The verification framework

A significant hurdle towards applying an effective verification methodology is the need for a good understanding of the system's architecture. A possible approach typically consists of decomposing the large-scale system into a "system of systems" and defining constructs from the interactions between the components, i.e., partition the problem into well-understood sub-problems; furthermore, capture the interactions between components and the system behaviors using appropriate computational tools. Traditionally, verification is carried out after the system design is implemented, which is referred to runtime verification or field-testing verification. Such an approach incurs high costs when error correction iterations are necessitated. A new approach, which consists of off-line verification and run-time verification as shown in Fig. 1, therefore, is dictated and pursued in parallel with the system design. In this approach, off-line verification is based on a system model in a suitable simulation environment, which aims to correct design errors at early stage of design. Runtime verification is then implemented on the prototype system to track and assess system performance on stability/availability, constraints satisfaction, optimization, and reconfiguration etc. In this configuration, the verification of offline verification is low-cost and it will reduce the number of iterations of costly runtime verification, and finally reduce the cost of system design.

Fig. 1 depicts the off-line versus runtime philosophy. By increasing the inexpensive error corrosion (N) in offline verification, we can reduce the costly error correction (M) in runtime verification to reduce design cost and timeline.

With this new approach, a generic verification framework needs to be introduced in order to address major complexity issues. The essential elements of the architecture include system analysis, specification definition, system modeling, and Monte Carlo simulations. System analysis investigates the system functions, decomposes high-level missions or activities into operations of different system components, and provides a list of failure modes. Specifications dictated by the customer/end-user or the designer are used to assess the system performance. Exhaustive tests are carried out via Monte Carlo simulations to ascertain that the system/model performs properly under all operating conditions. In this paper, the verification is considered in the context of automated contingency management, both normal and fault conditions need to be addressed considered. For the fault operating conditions, a fault injector is employed to simulate fault scenarios. The proposed verification framework is shown in Fig. 2.

By viewing a complex large-scale system through a hierarchical configuration, a layered off-line verification scheme is constructed. It is based on an implementation of a Failure Modes and Effects Criticality Analysis (FMECA) (Lu, Jia, Gao, & Han, 2013;

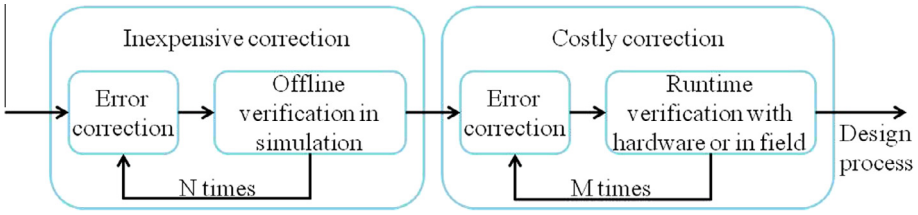

Fig. 1. The benefit of offline verification in a simulation environment.

دریافت فوری ← متن کامل مقاله

ISIArticles
مرجع مقالات تخصصی ایران

✓ امکان دانلود نسخه تمام متن مقالات انگلیسی
✓ امکان دانلود نسخه ترجمه شده مقالات
✓ پذیرش سفارش ترجمه تخصصی
✓ امکان جستجو در آرشیو جامعی از صدها موضوع و هزاران مقاله
✓ امکان دانلود رایگان ۲ صفحه اول هر مقاله
✓ امکان پرداخت اینترنتی با کلیه کارت های عضو شتاب
✓ دانلود فوری مقاله پس از پرداخت آنلاین
✓ پشتیبانی کامل خرید با بهره مندی از سیستم هوشمند رهگیری سفارشات