Transformation from AADL to Colored Petri Nets for Dynamic Reconfiguration Process

Lei Liu¹, Wei Zhao¹, Zeyong Jiang² and Shihai Wang²,³
¹Beijing Electro Mechanical Engineering Institute Beijing, 100074, P. R. China
liuleilarry@126.com; qiuahuabb@163.com
²School of Reliability and Systems Engineering, Beihang University, Beijing 100191, P. R. China
jiangzeyong0106@163.com; wangshihai@buaa.edu.cn
³Science & Technology on Reliability & Environment Engineering Laboratory, Beihang University, Beijing 100191, P. R. China

Abstract. Although integrated modular avionics (IMA) provides many advantages such as the reduced weight and higher efficiency for system operations, safety problems in IMA dynamic reconfiguration process come up due to its complexity to analyze. Architecture Analysis and Design Language (AADL) has advantage to model for embedded systems. However, it is quite limited to employ AADL for analyzing system safety. This paper, seeks to translate the AADL models of IMA dynamic reconfiguration process into colored petri net (CPN), which have advantages to simulate and evaluate embedded systems. Then, the colored petri net (CPN) is proposed for the analysis for AADL models, because CPN can describe the properties and behaviors of dynamic reconfiguration process well. Moreover, it is essential to make a transformation from the AADL models to the CPN models. This work will benefit the subsequent analysis of IMA dynamic reconfiguration process. Finally, a case study is provided for effectiveness the transformation rules.

1. Introduction
As a safety-critical system, The Integrated Modular Avionics (IMA) system takes the advantages of higher efficiency with less weight. Compared with federated systems, IMA systems support complex and flexible resource sharing, which is inherent on the IMA platform [1].

In this paper, dynamic reconfiguration refers to configuration changes conducted when failure occurs during flying. Dynamic reconfiguration can help in creating new backup areas to restart an application, which makes the plane more flexible and utilizes the hardware resources more effectively. Thus, modeling and analyzing IMA dynamic reconfiguration process ensure safety of IMA, when failure occurs in the flight.

The IMA system is a real-time embedded system [2]. The Architecture Analysis and Design Language (AADL) [3] is an SAE International (formerly known as the Society of Automotive Engineers) standard (SAE AS5506), based on Model-Driven Engineering (MDE). AADL is widely applied in embedded systems, especially in aerospace filed [4]. Zhang F [3] applied AADL to model F-16 ‘Auto Pilot Controller’ and analyzed the behavior properties of liveness and trace refinement with various fairness assumptions, considering time capacities and deadlines. Zhao Z [1] built an AADL model for the complex hardware structure and robust software of avionic display system. All of these features make AADL a good method to describe the transition process of a system, for example, the dynamic reconfiguration of IMA.
However, AADL is only a semi-formal model, and it is not mature for reliability analysis [5]. If there is need to analyze or evaluate complex systems, it is convenient to transfer into other models [6], such as Petri Nets, EDA (Event-Data Automata), etc. Petri Nets are a formal graphical and mathematical tool [7], capable of modeling and analyzing the dynamic behavior of systems [8]. They are also increasingly used for system safety, reliability and risk evaluation.

Therefore, in this paper, AADL is proposed to model the IMA dynamic reconfiguration process. Then, the colored petri net (CPN) is proposed for the analysis for AADL models, because CPN can describe the properties and behaviors of dynamic reconfiguration process well. Moreover, it is essential to make a transformation from the AADL models to the CPN models.

The remainder of the paper is organized as follows. Section 2 introduces the IMA dynamic reconfiguration process, AADL and CPN. In section 3, AADL is introduced to model IMA dynamic reconfiguration process. At the same time, transformation rules from AADL models to CPN models are shown. Moreover, section 4 comes with a case study about IMA dynamic reconfiguration process. Finally, the conclusions are made in section 5.

2. IMA Dynamic Reconfiguration Process

1) MA dynamic reconfiguration process

The IMA system is a complex system that has more open architectures, more widespread integration, more integrated functions, and high coupling between modules. Many challenges also appear when reconfiguration occurs. Dynamic reconfiguration in this study pertains to software. Then, the architecture of IMA software is introduced in this paper. The IMA system includes the IMA core system and noncore equipment according to the ASAAAC standard. The IMA core system contains several avionic racks. These racks contain CFMs and communication nets between them. Moreover, the racks have functional applications based on hardware, the operational system, and system management software.

2) AADL

AADL is an effective modeling tool for analyzing real-time embedded systems and complex systems. In this study, AADL was employed to model the process of dynamic reconfiguration of IMA.

There are three kinds of components in the AADL standard: Software components are used for the software architecture modeling which includes data, thread, thread group, process, and subprogram; Execution platform components are used for hardware architecture modeling such as processor, virtual processor, memory, bus, virtual bus and device; Hybrid components are used for modeling hierarchically.

3) CPN

CPNs are a high-level Petri nets used for designing, specification analysis, validation, and verification [66,67]. A CPN is a tuple $CPN = (\Sigma, P, T, A, N, C, G, E, I)$ [68], where: $\Sigma$ is a finite set of non-empty types, also called colour sets; $P$ is a finite set of places; $T$ is a finite set of transitions; $A$ is a finite set of arcs; $N$ is a node function; $C$ is a color function; $G$ is a guard function; $E$ is an arc expression function; $I$ is an initialization function. CPNs can describe the states of complex systems and state changes, due to triggering events. The feature of a CPN is that it provides a definition of color sets. A color set attached to a place has tokens in it. Each token should have a color. The guard of a transition needs to be satisfied before the transition is conducted.

3. Modeling and Transformation

3.1. Modeling of Dynamic Reconfiguration Process

AADL is introduced above to describe the IMA system. A mode of a system can be associated with the logical configurations. Mode transitions imply that the configuration state changes from one to another. A system or a component has different static structures and properties in different modes. A property can describe task scheduling, real-time characteristics, communication, memory, etc. Then, modes at the system level represent the content of a system configuration. A system has its own modules, partitions, processors, and communication bus in each mode. Thus, the static structure of the system in one mode is built by ARINC 653 annex in AADL.
A typical process of IMA dynamic reconfiguration is presented in figure 1. The arrows indicate that messages are being sent during the process. Rectangles represent the important actions that occurred. Compared with the reconfiguration process mentioned in another study that always has redundant modules, dynamic reconfiguration discussed in this study refers to a system without spare modules, especially when reconfiguration in the case redundancy is not designed or is used in the system when dynamic reconfiguration begins.

3.2. Rules of Transformation

The AADL model of IMA dynamic reconfiguration is effective in describing the system structure and complex reconfiguration process. Some analysis can be conducted in tools for AADL, such as Open Source AADL Tool Environment (OSATE). However, automatic simulation and analysis are not the strong points of AADL, but fit for Petri net. Meanwhile, there are also disadvantages in modelling embedded systems for Petri nets. In this study, modes in AADL model could be presented by places in CPN. Active modes in AADL could be presented by place with specific color token in CPN. Transitions of modes in AADL model could be converted into transition of tokens in CPN. Time properties of the state transitions in AADL model correspond to time stamps of tokens in arcs in CPN.

![Figure 1](image1.jpg)

**Figure 1.** A typical process of IMA dynamic reconfiguration process.

![Figure 2](image2.jpg)

**Figure 2.** The transformation rules from AADL model to CPN model.
The resources such as memory and data in AADL model that are shared in the system can be represented by tokens in a place in CPN. Finally, the constraints about memory and time in AADL model can be converted to guard functions in a Petri net. Therefore, AADL model can be translated into CPN integrally as shown in figure 2.

4. Case Study
In the case of the IMA system, a series of functional modules including navigation, display, communication, and integrated radio frequency sensors (IRFS) are integrated. The navigation module provides the place of the plane and guides the plane in a definition router. The module for an aircraft cockpit display provides the man–machine interface for a pilot. The communication module is responsible for the communication between an aircraft and a ground unit. IRFS integrates all the RF sensors in the aircraft for sending and receiving signals at all frequency ranges.

![Figure 3. The model of IMA system structure based on AADL.](image)

![Figure 4. The CPN model for the dynamic reconfiguration after transformation from AADL model.](image)
The configuration state of a system can be described by AADL. The logic configuration structure needs the ARINC 653 annex in AADL. The ARINC 653 entities fabricated using the system architecture correspond to the AADL components. The model of the IMA system is presented in a graphical manner based on AADL, as shown in figure 3.

Based on the rules defined in section 3, the AADL model of dynamic reconfiguration is converted to CPN. The modes and states of the behavior annex are converted to places in CPN. Mode transitions and behavior annex transitions are converted to transitions in the CPN. Other resources such as memory and data are represented by the color set of tokens in places. The triggering condition and constraints are added to the CPN as guard functions for a transition.

In this case, the system creates a new partition on module D that is defined as a substate in the behavior annex. Before the state is activated, the tokens pertaining to memory and to convey the message that the former state is completed should be send to transition. Moreover, the guard function in the transition must be satisfied. The CPN model is presented in figure 4. This is the basis of the subsequent analysis and evaluation of IMA dynamic reconfiguration process, based on CPN model.

5. Conclusions
IMA dynamic reconfiguration process brings great flexibility and reduces redundancies of the system. However, it also increases the complexity to analyze and evaluate. Therefore, in this paper, AADL is applied to model the IMA dynamic reconfiguration process. The relative transformation rules from AADL model to CPN model are proposed as well, since CPN models have advantages of simulation and evaluation, while AADL models have limits in these aspects. It can benefit the subsequent analysis and evaluation about dynamic reconfiguration of IMA system as the foundation.

6. Acknowledgments
This work was supported by the Defense Industrial Technology Development Program (JCKY2016204A102) and Foundation of No.61400020404.

7. References
[1] Zhao Z, Zhang J, Sun Y and Liu Z 2018 Conf. on The 30th Chinese Control and Decision Conference (Shenyang: China) pp 4121–4126
[2] Li Z, Wang S, Zhao T and Liu B 2016 J. Chin. J. Aeronaut. 29 1027–1041
[3] Zhang F, Zhao Y, Ma D and Niu W 2007 J. IEEE Access. 5 27421–27438
[4] Yang Z, Hu K, Ma D, Bodeveix J, Pi L and Talpin J 2013 J. Syst. Softw. 93 42–68
[5] Sendall S and Kozaczynski W 2003 J. IEEE Softw. 20 42–45
[6] Cuadrado J, Guerra E and de Lara J 2017 J. IEEE Trans. Softw. Eng. 43 868–897
[7] Bugarin A and Barro S 1994 J. IEEE Trans. Fuzzy Syst. 2 135–150
[8] Wieland C, Schmid O, Meiler M, Wachtel A and Linsler D 2009 J. J. Power Sources. 190 34