Chinese Journal of Aeronautics, (2016), 29(4): 1027–1041

Chinese Society of Aeronautics and Astronautics
& Beihang University

Chinese Journal of Aeronautics

cja@buaa.edu.cn
www.sciencedirect.com

A hazard analysis via an improved timed colored petri net with time–space coupling safety constraint

Li Zelin, Wang Shihai *, Zhao Tingdi, Liu Bin

Science and Technology on Reliability and Environmental Engineering Laboratory, School of Reliability and Systems Engineering, Beihang University, Beijing 100083, China

Received 15 September 2015; revised 16 February 2016; accepted 19 March 2016
Available online 23 June 2016

KEYWORDS

Petri nets;
Real-time systems;
Resource allocation;
System modeling;
Time–space coupling safety constant

Abstract Petri nets are graphical and mathematical tools that are applicable to many systems for modeling, simulation, and analysis. With the emergence of the concept of partitioning in time and space domains proposed in avionics application standard software interface (ARINC 653), it has become difficult to analyze time–space coupling hazards resulting from resource partitioning using classical or advanced Petri nets. In this paper, we propose a time–space coupling safety constraint and an improved timed colored Petri net with imposed time–space coupling safety constraints (TCCP-NET) to fill this requirement gap. Time–space coupling hazard analysis is conducted in three steps: specification modeling, simulation execution, and results analysis. A TCCP-NET is employed to model and analyze integrated modular avionics (IMA), a real-time, safety-critical system. The analysis results are used to verify whether there exist time–space coupling hazards at runtime. The method we propose demonstrates superior modeling of safety-critical real-time systems as it can specify resource allocations in both time and space domains. TCCP-NETs can effectively detect underlying time–space coupling hazards.

1. Introduction

With the development of computer and software technology and incremental increases in reliability, availability, and safety requirements for safety-critical real-time systems, the concept of partitioning in time and space domains is proposed in avionics application standard software interface (ARINC 653).[1] Multiple applications of different software levels share resources and are hosted on one common hardware platform. Applications are isolated by time and space partitioning to efficiently prevent fault propagation. Current operating systems with the ARINC 653 standard include: VxWorks653, LynxOS-178, and Integrity-178B. This paper will introduce time–space coupling safety issues in resource configurations mainly based on an integrated modular avionics (IMA) system.

An IMA architecture provides a shared platform with reusable and flexible hardware and software resources.[2] By replacing numerous separate, centralized common processing modules, IMA architectures benefit from low

* Corresponding author. Tel.: +86 10 82313598.
E-mail address: wangshihai@buaa.edu.cn (S. Wang).

Peer review under responsibility of Editorial Committee of CJA.

http://dx.doi.org/10.1016/j.cja.2016.04.016
1000-9361 © 2016 Chinese Society of Aeronautics and Astronautics. Production and hosting by Elsevier Ltd.

power consumption and maintenance savings, but bring with them potential safety issues.[3] The platform can host avionics functions of various safety levels while ensuring the integrity of the system through its robust partitioning mechanism. Time and space partitioning is the core concept of an IMA system. This type of partitioning requires adequate temporal resources (time slots) and spatial resources (memory space) to be allocated to each partition in the design phase in order to ensure proper execution and satisfy real-time constraint requirements. System designers usually configure time slots and memory space of each partition separately, ignoring time–space dynamic connection requirements between partition resources, which are heavy, complicated, and error-prone.[4] Spatial resource requirements of applications vary from and can be affected by their allocated temporal resources. The interactive relationship between temporal and spatial resources introduces new safety issues.

Petri nets (PNs) were first introduced in the doctoral dissertation, "Communication with Automata", of Carl Adam Petri.[5] PNs are an information flow model of network structure with parallelism, uncertainty and synchronism. PNs provide formal methods to establish mathematical models that can describe system behaviors and also provide a graphical interface that helps system modeling and analysis.[6] PNs have been proven to be effective graphical, mathematical modeling and analysis tools that are widely used to model asynchronous, concurrent computer systems. PNs have been expanded and contain different features and functions for specific modeling purposes such as timed PNs[7], colored PNs[8], and hierarchy PNs.[9] For analyzing time–space coupling hazards in safety-critical real-time systems, all of these current methods seem unsatisfactory. To deal with resource coupling in a time–space domain, this paper proposes a time–space coupling safety constraint. Furthermore, a new, timed colored Petri net with time–space coupling safety constraints (TCCP-NET) is introduced and employed for time–space coupling hazard analysis.

This paper is organized as follows: Section 2 – a brief introduction of classical PNs, colored PNs, timed PNs, their modeling and analysis methods, and limitations. An IMA system, as an example, is introduced to illustrate the concept of time–space partitioning where time–space coupling hazards are possibly introduced; Section 3 – specifications of time–space coupling and time–space coupling safety constraints; Section 4 – a new, timed colored PN is proposed with time–space coupling safety constraints. Its modeling process and analysis methods are introduced; Section 5 – a case study and discussion are used to demonstrate the effectiveness of the proposed modeling and analysis methods; Section 6 – conclusion and future work.

2. Background

2.1. PN

2.1.1. Classical PN

A classical PN[10] has two different types of nodes: places (circles), transitions (rectangles). The different nodes are connected by directed arcs (arrows). A place can contain any number of tokens, and the distribution of tokens over places is called a marking, which represents the allocation of resources. If all input places connected to a transition have more than one token, that transition can be fired. Tokens in input places are removed and tokens are generated in output places. Any transition in a PN may be fired concurrently if it is enabled. Due to uncertainty and concurrency, there are many distributions of tokens that represent various markings.

Table 1 Interpretations of places and transitions.[11]

Input place	Transition	Output place
Required resources	Tasks	Freed resources
Input data	Computations	Output data
Input signals	Signals processing	Output signals
Buffers/registers	Processors	Buffers/registers

In the modeling process, the state of a system is generally denoted by places, and behaviors that change system state are denoted by transitions. Some typical interpretations of transitions and their input places and output places are shown in Table 1.

Complex behaviors in the system can be modeled by a classical PN. The model is then used to analyze behavioral and structural properties of the system.[12] However, a number of limitations exist in this type of PN:

(1) All tokens are identical and descriptions of resource types are too simple.
(2) It is difficult for existing attributes in PNs to describe additional system properties.
(3) The concept of time is not taken into consideration in the modeling and simulation process.

2.1.2. Timed PN

The timed PN (TP-NET)[13] is derived from classic PNs. It models interactions between activities, taking into account time properties. Time is introduced into a TP-NET in different ways:

(1) Time associated with tokens. Each token is associated with a time value that indicates when the token is available to fire a transition.
(2) Time associated with arcs. Each arc is associated with a delay t, which indicates a token takes t time to travel between two nodes.
(3) Time associated with transitions. Each transition can be associated with a delay t or delay interval [start, end], which represents time required to fire a transition.

With such time properties, TP-NETs have been widely used for modeling and performance evaluation, especially in real-time systems.[14–16]

The structure of a TP-NET is $N_{\text{timed}} = (P, T, A, W, M_0, I)$, where $N = (P, T, A, W, M_0)$, a marked PN. Symbols P, T, A, and W represent places, transitions, arcs and initial marking respectively. $I(t)$ denotes firing time of a transition and is called the firing time function.

The TP-NET specifies how much time an individual operation takes and how long it is necessary wait before it is ready. In TP-NETs, powerful time properties can help model time-dependent system behaviors that can be used in simulation to analyze problems in a time domain.