Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Engineering 29 (2012) 1060 – 1065

Procedia Engineering

www.elsevier.com/locate/procedia

2012 International Workshop on Information and Electronics Engineering (IWIEE)

Agent-based Simulation Framework for Safety Critical System

Zhu Yujun*, Xu Zhongwei, Mei Meng

Tongji University, No. 4800 Cao'an highway, Shanghai ,201804, China

Abstract

Safety critical Systems often integrate multiple complex functions and must generally ensure safety. These requirements lead to a need for simulation system that provides a prototype system for evaluation. This article proposes an agent-based simulation framework to meet the challenges of designing and evaluating the performance of the safety critical system. The approach proposed represents each agent architecture including Agent communication interface, Reasoning, Modeling, domain knowledge set, Execution and human agent interface units. The agent maps the safety requirement using risk ordering. The whole simulation system composed of multiple agents. One case study shows that agent-based simulation can express the behavior and performance of the system as a whole, especially, safety attributes can be displayed.

Keywords: Safety critical system; Agent; Simulation Framework;

1. Introduction

In the real world, safety critical systems are being studied actively and extensively in both academia and industry because major failures lead to highly undesirable outcomes. After having realized such system, designers normally need to develop a prototype system for evaluation. Computer simulation is an attractive approach to evaluate real-world systems by means of imitating system operations numerically and computing various performance measures. A validated simulation system is a potentially valuable tool for comparing system alternatives. It is hard to build a simulation system that can represent the real system with the similar behavior or the attribution, especially, depict the safety attributes.

* Corresponding author.
E-mail address:dyzhuyujun@163.com.

1877-7058 © 2011 Published by Elsevier Ltd.
doi:10.1016/j.proeng.2012.01.089

2. Challenges of Simulation

Due to the considerable complexity and instantaneity in safety critical systems, their simulation models are absolutely intensive. A series of challenges which we have adapted to the realm of safety critical system must be met[1][2].

2.1. Precise representation of the real system

A validated simulation system must properly model the real system. The simulation modeling can represent the structure, behavior and attribute of the actual system, especially, functionalities are introduced into the model at each step that the integrated component reliably represents the part of the real system being modeled.

2.2. Composability

Each safety critical system almost is complex, designers always decompose the overall functions of the system into sub-functions in order to partition the search space for sub-systems and components .The whole system is a set of interacting composable components, which cooperatively achieve the overall system function. And therefore, composability is still a major subject in modeling and simulation. Although composability is taking more and more interest in modeling and simulation, its implementation is not without difficulties.

2.3. Communication and coordination

To accomplish a goal or adapt to changing circumstances in the environment, Communication and coordination is needed between the various simulation components. However, the availability of a system is so critical that having to stop it even for a short time is unacceptable, and external environment is always changing. Simulation components must be capable of communicating and engaging in cooperative tasks in real time.

2.4. Safety

There is the challenge associated with safety in the implementation process. Simulation must be consider the safety functions which control the recognized hazards to achieve an acceptable level of risk and take the form of being protected from the event or from exposure to something that causes health or economical losses. So far it is difficult to express the safety attributes in simulation model.

3. Agent Architecture Design

Firstly, we will briefly introduce what is the component. A component is a software module that performs a defined task. Components, when combined with other software components, can constitute a more robust piece of software that is easily maintained and upgraded. Components interact with one another through various communication mechanisms. The agent architecture of safety critical system, We propose, is a highly component-based (modular) architecture[3].

Each component in our agent architecture can communicate information to/from all other components as needed through a communication mechanism including message format and message protocol. In order to facilitating the sharing of data/information among agents, we use a common agent communication