

# High Assurance System for Tokyo Metropolitan Area Railway Network

Kazuo Kera

Hitachi Ltd., Japan

E-mail; kazuo\_kera@pis.hitachi.co.jp

## I. Introduction

Large-scale public systems in today's information control field require that several conditions should be satisfied. First, a phased-in construction of the system must be possible so that the system can be constructed over a long period of time. Second, the system must be flexible and be adapted to meet the changes of social needs. All such systems are assumed to constantly grow, expand and change. We must modify the system in order to grow it; however, its reliability may be reduced by every modification. In the case of a conventional system, where it is assumed that there will be no growth, reliability is assured if the system is reliable when introduced. On the other hand, a growing system has the major problem of stable operation without reduction of reliability even as it is routinely modified. A system that can grow and operate stably with high reliability is called a high assurance system; the technology it uses is called assurance technology.

## 2. High-Assurance System Technology

Autonomous Decentralized System (ADS) architecture has been used mainly to realize high assurance computer systems in control systems field. Information Technology has developed remarkably in recent years, and the systems have many high functions. For example, a control system supplies not only conventional control function, but also various information services and other heterogeneous functions. For such growing large-scale system in which heterogeneous functions co-exist, the mechanism to protect mutual violation from each other should be required. And the mechanism to minimize the effects to the existing functions should be necessary. Furthermore the mechanism to protect online system from test

system's violation should be also necessary when the system is changed. We are constructing a high-assurance, large-scale railway transport operation control system in which heterogeneous functions coexist. We have expanded the conventional ADS architecture and realized phased-in system construction and online system expansion, which are important items in assurance technology.

In this presentation, we will clarify the requirements for high assurance system including heterogeneous needs (different functions and different operation modes). The requirements are the realization of system change that can be implemented flexibly with few effects to other online system, and the reduction of risk factors that lower the reliability and quality of a growing system when the system is changed. We will then examine the assurance technologies to achieve these needs.

## 3. Application to ATOS for Tokyo Metropolitan Area Railway Network

We will show the results of the application of assurance technology to a large-scale Tokyo metropolitan transport operation control system ATOS, which covers Tokyo metropolitan area railway network including 17 lines and 250 stations in high-density traffic. The utilization of this area is 15 million people per day. The key system realizing safe and punctual railway services is ATOS, consisting of total 2200 de facto-standard computers including Workstations, PCs and small servers. We will also describe the phased-in system construction method with concrete examples, the results and evaluation, as evidence that assurance technology is very effective.

(ATOS; Autonomous Decentralized Transport Operation Control System)