Development of High-performance Platform for Onboard Signalling Systems to Ensure Railway Operation Safety

With railways having attracted attention over recent years as a means of transportation suitable for sustainable societies, the wider adoption of railway systems around the world is expected to continue into the future. In parallel with this, Hitachi, Ltd. has experience developing platforms for onboard signalling systems that are based on its own proprietary safety mechanisms in order to provide the high levels of safety and processing performance required for this application. These platforms have been deployed in railway onboard signalling systems around the world. With the rising demand over recent years for the miniaturization and performance enhancement of onboard signalling systems, however, Hitachi has now developed a new high-performance platform for this purpose. This article describes the development of this new platform.

Masayuki Miyaji
Kosuke Onishi
Kazuki Morita

1. Introduction

Hitachi, Ltd. has developed onboard signalling systems based on its own proprietary safety mechanisms and deployed them in railway signalling systems both in the Japanese market and farther afield. To deliver the high levels of safety and processing performance required by onboard signalling systems, Hitachi has also in the past developed a fail-safe central processing unit (FS-CPU)[*1] and platforms in which it forms a key part. These platforms have been used to implement onboard signalling systems, with the FS-CPUs running a dedicated operating system (OS) that in turn hosts applications that provide the functionality for signalling systems such as automatic train control (ATC) and the European Train Control System (ETCS).

With more than a decade having passed since the development of the current FS-CPU, however, Hitachi recognized that higher processing performance would be needed on the new platform in order to implement the functions required by the latest signalling systems, such as radio communications and the ability to operate with higher traffic densities. Furthermore, while some instances of the existing platform used system configurations with multiple FS-CPUs to overcome performance constraints, the consequent larger overall size of the onboard signalling system hardware caused problems with occupation of the installation space on rolling stock.

It was these factors that led Hitachi to develop its new high-performance platform for onboard signalling systems with the objectives of improving performance and reducing the size of the system through hardware consolidation. Along with use of the newly developed FS-CPU to boost performance, the project also included the development of an OS to run on the FS-CPU, enabling the concurrent execution of multiple applications on a single CPU without

*1 A large-scale integration (LSI) device that ensures a high level of safety by having two CPUs perform the same operations and using a comparator to compare execution results of the two CPUs.

compromising safety. The platform was audited for compliance with European safety standards by an independent safety assessor (ISA) who certified it as achieving Safety Integrity Level 4 (SIL4). This article describes the development of the new high-performance platform.

2. Development Concept

As noted above, the development objectives were to improve the performance of the onboard signalling system and to reduce the system size through the consolidation of hardware. To achieve the objectives, the platform development adopted the following measures (see **Figure 1**). Details of each of these are provided in the following sections.

(1) Development of new FS-CPU for higher performance

Hitachi developed a new FS-CPU to provide higher processing performance while still maintaining the same high safety level as the previous FS-CPU.

(2) Development of OS capable of concurrent execution of multiple applications

To complement the enhanced performance of the FS-CPU, a new OS was developed to enable the concurrent execution on the same CPU of functions that were implemented on separate devices under the previous configuration.

(3) Hardware size reduction through circuit redesign

The platform for onboard signalling systems was built using the above FS-CPU and software to consolidate hardware. Moreover, the hardware circuits were also redesigned to reduce unit size.

2. 1 Performance Improvements Achieved by Development of New FS-CPU

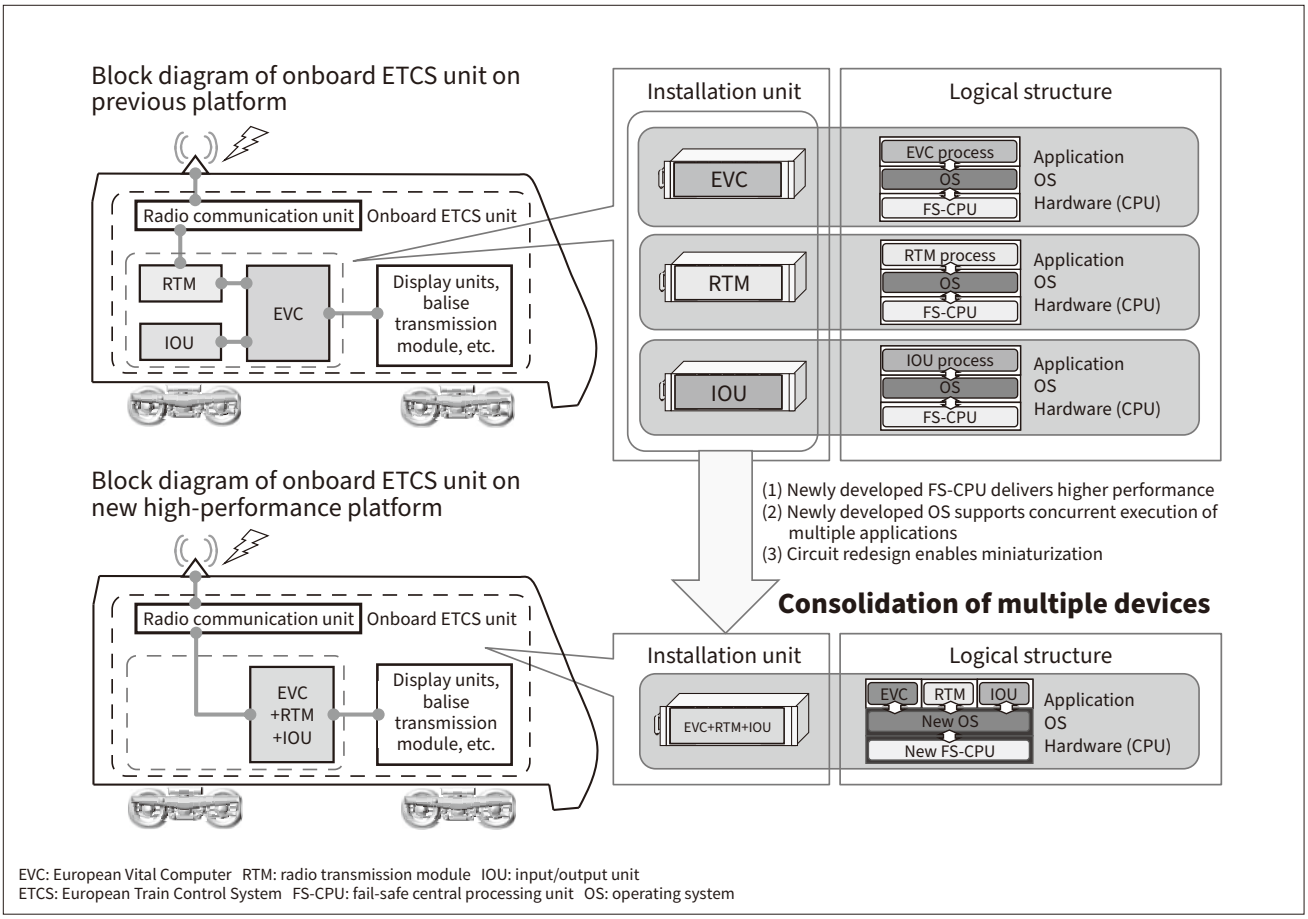
Prior to developing the new platform, Hitachi first developed and deployed a new FS-CPU that provided higher processing performance while still maintaining the same high safety level as the previous FS-CPU.

The FS-CPU is an LSI device containing two CPUs and a comparator that compares the two CPUs' execution results to detect CPU miscalculation.

Like the previous model, the new FS-CPU is a single-chip device that integrates two CPUs and a comparator that compares the input and output data of the CPUs. On the other hand, a four-fold increase in processing performance was achieved compared with the previous model by

Figure 1 — Development Concept of New High-performance Platform

The new high-performance platform was developed to be smaller in size by consolidating functions that on the previous platform had a distributed implementation.



EVC: European Vital Computer RTM: radio transmission module IOU: input/output unit
ETCS: European Train Control System FS-CPU: fail-safe central processing unit OS: operating system

updating the operating frequency of the CPUs and system bus. An Ethernet communication function is implemented on the new FS-CPU equipped with four Ethernet port and communication buffers. The function eliminates the need for the platform to have a separate network interface board, which is required in the previous model. The operation of the comparator is synchronized with the bus cycle to enable detection of a failure in the comparator itself. Moreover, the application of strict layout and routing rules to the chip circuit and mounting design minimized the risk of common cause failures. The use of error-correcting codes (ECCs) in the large random-access memory (RAM) and cache also plays an important part in ensuring a high level of safety and reliability in the onboard signalling system.

2. 2
Development of New OS to Achieve Equipment Consolidation

The software on existing onboard signalling systems took the form of applications and an OS. Applications provided the functionality for the relevant signalling system such as ATC or ETCS, and the OS handled hardware control in response to requests from the applications. Hitachi developed a new OS for the new platform to enable the concurrent execution on a single FS-CPU of functions that were implemented on separate devices on the previous configuration. To enable this concurrent execution to be achieved without compromising safety, the new OS manages, monitors, and controls the onboard signalling system applications in ways that address the following three concerns.

(1) Prevention of CPU resource occupation by failed application

The OS operates the applications to be executed periodically at a fixed time. When the OS is operating multiple applications, and if an application does not complete its processing within the fixed time, the application continues to occupy the CPU and disturbs the execution of subsequent applications. The new OS monitors the applications periodically and stops only the application that is diagnosed as faulty so that excludes it from the execution target of the subsequent operation. Thereby, the OS ensures execution time available for subsequent applications and degraded operation will be performed (see **Figure 2**).

(2) Function to handle failure of individual applications

The consolidation of functionality into a single device requires the OS to isolate particular applications from operation when the applications are detected as faulty. The

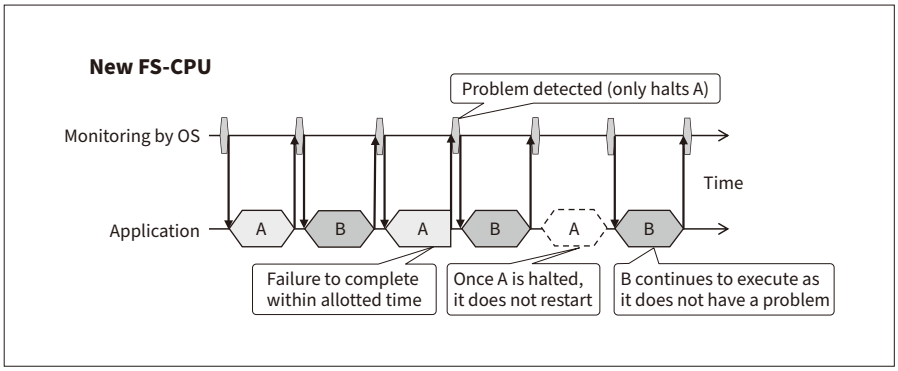


Figure 2 — Operation of Software on New FS-CPU

The diagram shows the time-sequence for cyclic execution of the new OS and applications on the new FS-CPU. The new OS monitors each application at fixed time intervals. If a problem is detected on a particular application, the OS shuts down that application only. The diagram shows an example in which the OS detects that application A has failed to complete within its allotted time. The OS halts application A only and allows application B (which does not have a problem) to continue executing.

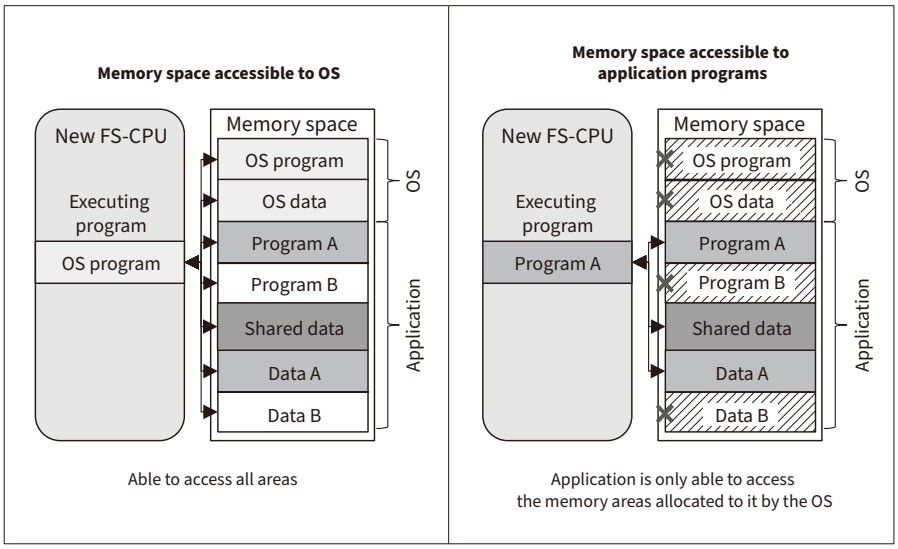


Figure 3 — Memory Areas Accessible to New OS and Applications

The new OS has access to the entire memory space to enable it to manage, monitor, and control both itself and the applications it is hosting. Applications, in contrast, only have access to the memory areas allocated to them by the OS, an arrangement that prevents them from inadvertently overwriting program or data belonging to the OS or other applications.

new OS provides each application with its own separate memory space so that it is able to halt a faulty application without interfering with the continued execution of other applications (see **Figure 2**).
(3) Prevention of faulty overwriting of program or data belonging to other applications

As memory management on the existing OS provided applications with shared access to the same memory space, there was a risk of their faulty overwriting of programs or data belonging to other applications. The new OS prevents this by providing each application with its own memory space and blocking access to other areas (see **Figure 3**).

2. 3
Platform Deployment and Hardware Miniaturization

Along with the main circuit board containing the FS-CPU and the OS, the new platform also includes peripheral interface boards for communications and for input and output to external devices such as the braking circuit on rolling stock.

The main CPU board of the platform mounts the FS-CPU that executes safety-related processing. The board sends safety-critical outputs such as brake commands via output circuits that utilize a dedicated bus with a dual configuration for safety. Interfaces to external devices that are not part of the platform, meanwhile, are implemented as peripheral circuit boards. These boards are connected to a general-purpose bus, thereby enabling a choice of boards to be used depending on which interfaces are needed by the specific application systems (see **Figure 4**).

In addition to making the platform more versatile and expandable, this also helps make systems smaller by only including circuit boards that are needed. Furthermore, the platform has extendibility to add interfaces that are required for a specific system application by applying specific interface boards compatible with the general-purpose bus together with application-specific drivers without changes to the main CPU board and the OS.

The miniaturization of components and revising the circuit design used in existing systems made the unit size smaller. In addition to the hardware consolidation made possible by the performance improvements described above, the equipment size was reduced by 50% compared to the previous model when applied to implement a European Vital Computer (EVC)[*2] for an onboard ETCS.

2. 4
Development Process and Safety Certification

The design and testing for this project were undertaken in accordance with the development processes stipulated in the European Norm EN50126[*3], EN50128[*4], and EN50129[*5]. The platform was audited by an ISA and certified that the platform complied with SIL4.

Figure 5 shows the steps and the scope of the certification acquired by the development project. The certification scheme that applied to current projects using the previous platform was conducted as either a generic application (GA)[*6] or as a specific application (SA)[*7] covering application systems based on the platform. The problem with this approach is that, even though the platform itself is applicable to several application systems, the resulting certification is not applicable to other applications.

Accordingly, development adopted a certification program for the platform that covered a generic product (GP)[*8] scope of certification (see **Figure 5**). This scheme involved

*2 Controller for onboard ETCS units that handle safety functions such as speed checking and brake control.
*3 European Norm for specification and demonstration of reliability, availability, maintainability, and safety (RAMS).
*4 European Norm for software for railway control and protection systems
*5 European Norm for safety-related electronic systems for signalling
*6 A system with functions for specific applications (such as application-specific operation)
*7 Systems for deployment of individual applications, including installation conditions
*8 Systems with generic applicability to different applications

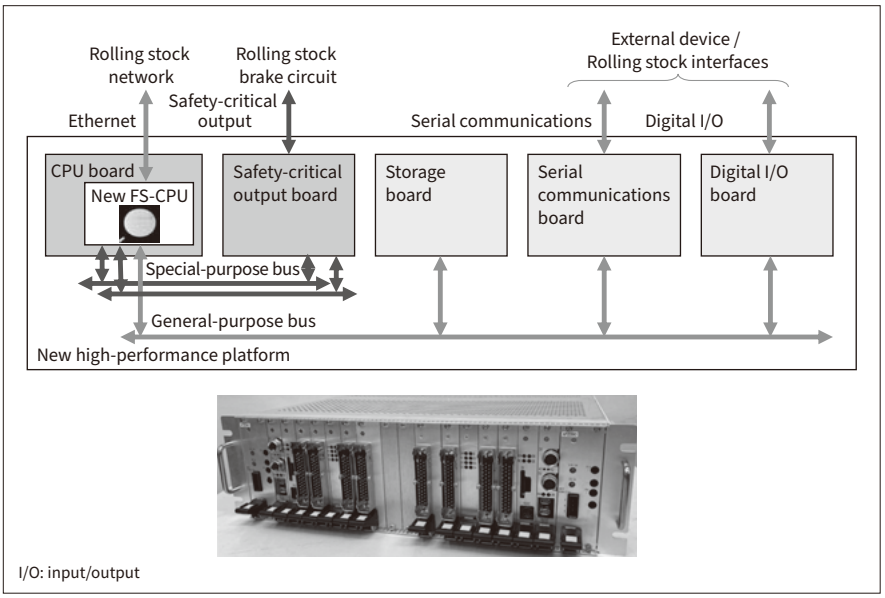
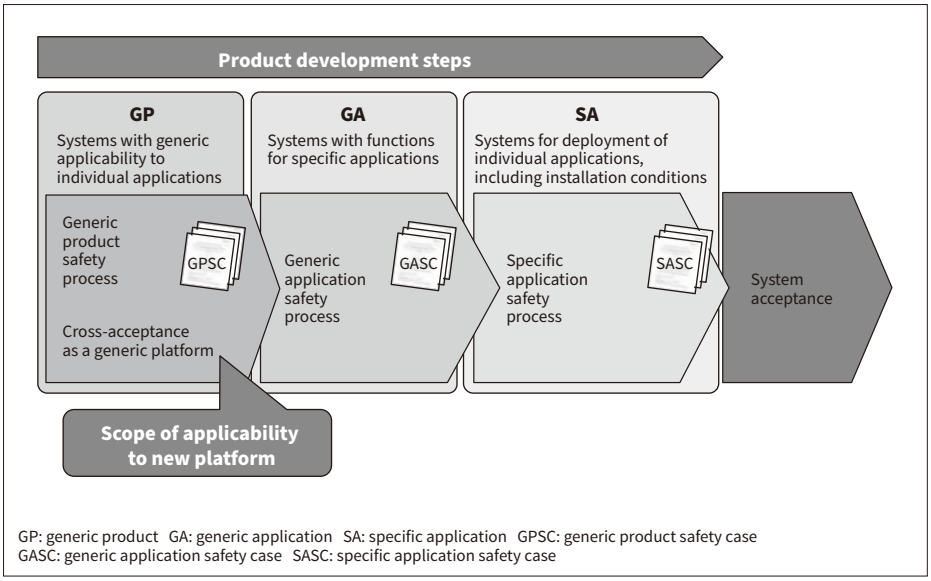


Figure 4 — New High-performance Platform and Hardware Configuration
The new high-performance platform is made up of the main CPU board, which contains the new FS-CPU, and peripheral interface boards that connect to the bus to provide the required functions. The photograph shows an EVC for an ETCS onboard system.

Figure 5 — Certification Steps and Scope of Application to New Platform

Safety certification is divided into three steps covering system development and deployment: GP, GA, and SA. The new platform has obtained GP safety certification with general applicability for subsequent product deployments (GA and SA).



identifying the safety and reliability requirements from specific application systems and designing the platform to satisfy these requirements. The safety constraints to be satisfied when the platform is integrated in a system are collated in safety-related application conditions (SRACs). The safety certification of the platform development is applicable for subsequent GA and SA certification provided that all SRACs are satisfied. The results of this certification were collated as a generic product safety case (GPSC) and audited by the ISA.

Meanwhile, the testing process verified and validated that the new platform was sufficiently reliable for use in actual rolling stock, with environmental testing being conducted in addition to the functional testing based on system requirements. This environmental testing was conducted with the system installed in EVC sub-racks and in accordance with European Norm covering things like temperature and humidity, vibration and shock, and electromagnetic compatibility (EMC).

3. Conclusions

This article has described the development of a high-performance platform for onboard signalling systems with the objectives of performance improvement and hardware consolidation. The work included the development of a new FS-CPU and OS. The new platform has also completed safety assessment and obtained SIL4 safety certification. Applications that perform the functions of onboard signalling systems used in Japan have been implemented for the platform and testing has verified that they satisfy the functional and performance requirements.

In the future, Hitachi plans to deploy applications for onboard signalling systems on this platform and roll out products to railway signalling systems in the Japanese market and elsewhere.

Authors

Masayuki Miyaji
JPN Products Development, Operations Signalling & Turnkey, Railway Systems Business Unit, Hitachi, Ltd.
Current work and research: Development of platform for onboard signalling systems.

Kosuke Onishi
JPN Products Development, Operations Signalling & Turnkey, Railway Systems Business Unit, Hitachi, Ltd.
Current work and research: Development of platform for onboard signalling systems.

Kazuki Morita
JPN Products Development, Operations Signalling & Turnkey, Railway Systems Business Unit, Hitachi, Ltd.
Current work and research: Development of platform for onboard signalling systems.