TAS Control Platform: A Platform for Safety-Critical Railway Applications

by Andreas Gerstinger, Heinz Kantz and Christoph Scherrer

Within the railway industry, the need for computer systems to perform safety-critical tasks is constantly increasing. A typical application is the railway interlocking system (Figure 1): these systems control the state of the signals and switches on railway lines and are therefore responsible for safe train operation. An incorrect output from such a system may in the worst case lead to a train collision. Other applications in the railway domain are axle counters along railway lines, computer systems on board trains, and field element controllers that operate under rough environmental conditions.

All these systems have an important common feature: they are safety-critical and must therefore be developed according to the highest safety integrity level (SIL4), as defined in the standards applicable to the railway industry (CENELEC 50126, 50128, 50129, Railway Applications Standards [RAMS, software and electronics]). Apart from being suitable for safety-critical operation, railway systems must also be highly reliable and available, and in most cases must meet stringent real-time requirements.

Due to the variety of applications with these common requirements, THALES Rail Signalling Solutions has developed a generic fault-tolerant computer platform that fulfils them, and thus enables the application programmers to fully concentrate on developing the correct application. Due to the increasing complexity of applications, it is also necessary that the platform be able to keep up with ever increasing demands for processing power, memory consumption and connectivity.

This trend can only be addressed by the use of off-the-shelf hardware and operating systems. In order to be able to keep up with the advances in hardware and operating systems, these components should be as interchangeable as possible, such that exchanging them does not compromise the system's safety integrity. For this reason, the middleware that implements the safety functions is strictly separated from the rest of the system. This layered structure can be seen in Figure 2.

Figure 1: Electronic interlocking for mainline rail.

The core hardware containing the CPU board and the interfaces represents the lowest level, and is cleanly separated from the rest of the system. This means that the hardware best suited for each purpose is utilized (eg for rail signalling systems powerful processors and a large amount of memory is needed, whereas for on-board systems low-end hardware with increased environmental resistance is preferred), and that CPU upgrades can be easily performed for new platform generations without major impact on the rest of the system.

The operating system is compliant with POSIX (Portable Operating System Interface), and is currently based on a microkernel. The next platform generation will be based on a more powerful operating system with a Linux kernel, which will bring benefits regarding hardware support and real-time performance.

The main innovation of the platform is its safety middleware, which is the decisive element that makes it suitable for safety-critical applications. The safety middleware ensures the clean separation of the lower levels (hardware and operating system) from the application, and provides all services to ensure safety. The safety middleware also provides the ability to run the platform in redundant configurations.

The applications on top of the layered architecture provide the actual services. The platform can be operated in three architecture variants (Figure 3). The 2oo3 ('2-out-of-3') configuration provides both the required level of safety

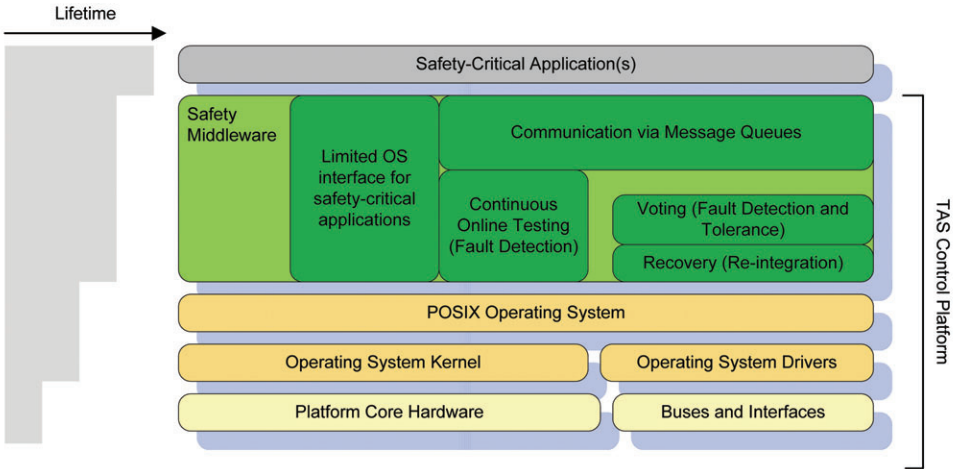
Lifetime
Safety-Critical Application(s)
Safety Middleware
Limited OS interface for safety-critical applications
Communication via Message Queues
Continuous Online Testing (Fault Detection)
Voting (Fault Detection and Tolerance)
Recovery (Re-integration)
POSIX Operating System
Operating System Kernel
Operating System Drivers
Platform Core Hardware
Buses and Interfaces
TAS Control Platform

Figure 2: TAS control platform layer structure.

and fault-tolerance mechanisms to enhance availability. In this configuration, all safety-critical decisions are subject to a majority voting procedure, such that a failure of one element is detected and tolerated. A 2oo2 configuration provides the same level of safety but a lower level of availability, since in the case of a conflict of output values between two elements, a failure of one element is detected but not tolerated, since it cannot be decided which one is correct. Finally, a 1oo1 configuration allows an application to be safely operated on a single hardware element, but requires the generation of a diverse application according to specified diversification rules. Software diversity ensures that the same level of safety is achieved.

The safety middleware layer (Figure 2) provides the communication services to globalize data amongst replicated hardware and thus ensures a consistent view even in the case that one replica is faulty and sends erroneous and inconsistent data messages. The API to access these services is implemented as voted message queues. An application transparent voting service enables the reliable detection of faults and the isolation of the faulty replica. This runtime environment for safety-critical applications also ensures replica determinism which is a prerequisite for software execution and voting on redundant hardware. In addition, the platform allows safety-critical applications to access only a limited part of the operating system API, so that replica determinism and safe execution within the runtime environment is guaranteed.

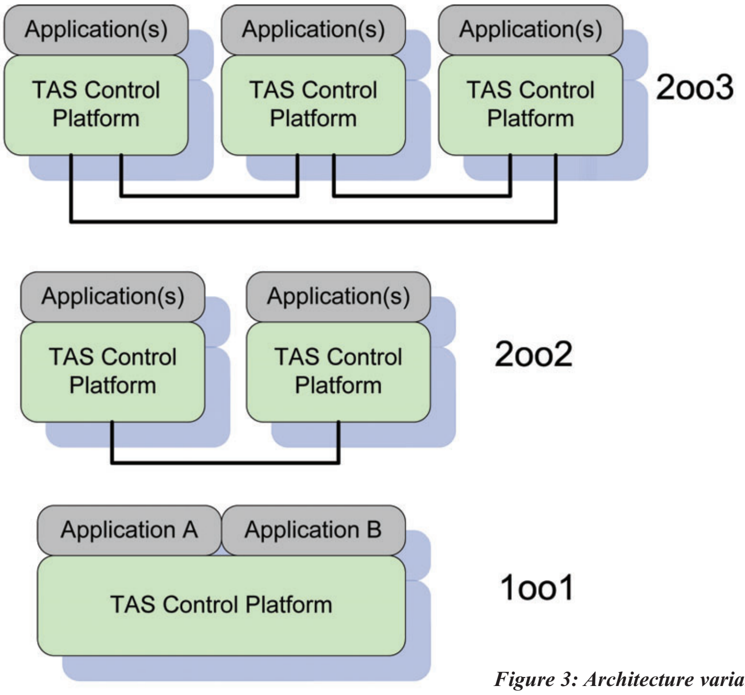

Figure 3: Architecture variants.

To ensure that no latent faults are aggregated in the hardware, the platform also performs continuous online testing of the hardware. This online testing, which is performed by a background task, covers the CPU, memory, buses, clocks and disks. Finally, the platform allows safety-critical applications to access only a limited part of the operating system, so that the safe execution environment of the application is guaranteed.

The platform, launched in 2001, is a well-established product and in operation in more than twenty countries on four continents. It has demonstrated that its safety and reliability approach fits for all vital railway applications within THALES Rail Signalling Solutions. To cope with rapid technology changes in hardware and software, functional enhancements and new concepts for fault detection and tolerance are currently being developed. The next generation of the platform will provide enhanced support for software and hardware diversity, to ensure that the same level of safety can be maintained in the long term with future hardware and software.

Links:
http://www.thalesgroup.com/markets/Activities/Ground-Transportation.html

Please contact:
Andreas Gerstinger, Heinz Kantz, Christoph Scherrer
Thales Rail Signalling Solutions GesmbH, Austria
E-mail:
andreas.gerstinger@thalesgroup.com,
heinz.kantz@thalesgroup.com,
christoph.scherrer@thalesgroup.com