SUCCESS STORY

➢ TRANSPORT ➢

With PolySpace Ada Verifier, CSEE Transport shifts into high gear

HIGH SPEED RAIL SIGNALING

For nearly a century, CSEE Transport has accumulated experience and know-how in rail and urban transport signaling systems: in 1902, the company equipped the new Paris subway! Today, as part of Ansaldo Signal NV, a subsidiary of the Italian Finmeccanica group, CSEE Transport has acquired the status of world leader in signaling and control-command systems for high-speed rail transport: via the French, Belgian, English and Korean TGV. The same is true for subway monitoring and control systems, the most recent being in Lisbon and the shuttles for the Channel Tunnel - linking England and France by rail under the English Channel. These successes are due in large part to CSEE's mastery of software technologies.

REQUIREMENT: ZERO-DEFECTS

When high-speed TGV trains run at 300 km/h, and two trains are separated by just three minutes - which is the case for example in France - any minor signaling malfunction would be fatal. For fast trains such as the Paris subway, CSEE Transport is subject to security norms as strict as those imposed in the nuclear industry. For this reason, the company is constantly on the lookout for the most advanced validation techniques available for software dependability.

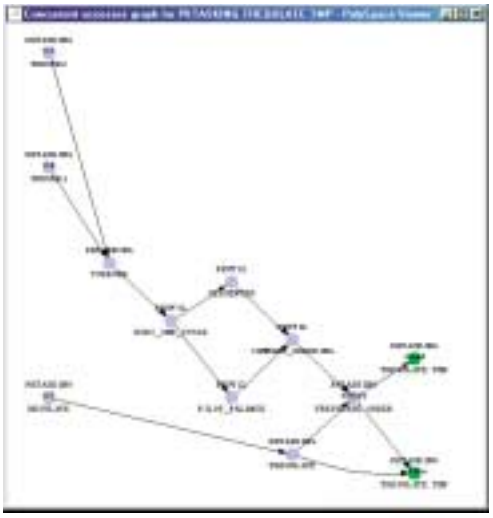
15 000 LINES OF CODE VERIFIED IN A FEW HOURS

A high-speed TGV signaling system is composed of ground-based equipment - a signal is placed every 14 kilometers -, and an embedded, on-board software application. The ground-based equipment automatically calculate the train's "halting sequences" (momentary halts, acceleration or deceleration) according to their position. This information is transmitted via the rails, processed by the on-board computer and displayed on the operator's screen. With no counter-command from the operator, the computer executes the commands automatically.

PolySpace TECHNOLOGIES

« POLYSPACE ADA VERIFIER CORRESPONDS PERFECTLY TO OUR NEEDS »

The security software for such a signaling system requires 15 000 lines of code, written in Ada.
This represents approximately one year's work, to which must be added three to four months of verification: re-reading source code, security analyses (simulation, constraints verification). PolySpace Verifier provides an exceptional aid. Re-reading source code, for example, a long and difficult task, is now automated. This lightens the workload for the specialists in charge of security, who now focus on problems that cannot be handled automatically.



WHY USE POLYSPACE ADA VERIFIER?

PolySpace Ada Verifier allows the verification of software without execution. At CSEE Transport, the tool now serves to identify access to non-initialized variables, division by zero, out-of-bounds array access.
It also signals sources of errors undetectable by classical verification: concurrent access by parallel tasks to shared variables. In particular, say the developers at CSEE Transport, it can be used at each step in software development, to validate the different modules before final integration.

PolySpace TECHNOLOGIES

Email: contact@polyspace.com
www.polyspace.com