

CSEE Transport Ensures Reliability of High-Speed Rail Software with PolySpace™ Products for Ada

As part of Ansaldo Signal NV, a subsidiary of the Finmeccanica group, CSEE Transport is a world leader in signaling and control-command systems for high-speed rail transport. The TGV (train à grande vitesse, or “high-speed train”) in France relies on CSEE Transport technology, as do Belgian, English, and Korean TGV trains. CSEE Transport also develops subway monitoring and control systems and the shuttles for the Channel Tunnel, which links England and France by rail.



High-speed TGV train.

In France, high-speed TGV trains operate at 300 kilometers per hour and run just three minutes apart. In this environment, even a minor signaling malfunction can be disastrous. Because passenger safety is paramount, software reliability and security are a top priority. For fast trains such as the Paris subway, CSEE Transport is subject to security regulations as strict as those imposed in the nuclear industry.

To ensure safe operation of the trains, CSEE Transport engineers often spend months verifying their code. CSEE Transport used PolySpace™ Client for Ada and PolySpace™ Server for Ada to automate tasks in this labor-intensive process and detect a wide range of run-time defects.

THE CHALLENGE

A high-speed TGV signaling system is composed of ground-based equipment placed every 14 kilometers and an embedded, onboard software application. The ground-based equipment automatically calculates

the train’s “halting sequences” (momentary halts, acceleration, or deceleration) according to its position. This information is transmitted via the rails, processed by the onboard computer, and displayed on the operator’s screen. Unless there is a counter-command from the operator, the computer executes the commands automatically.

The security software for CSEE Transport’s signaling system was developed in Ada in about one year. After the initial development phase, the team expected to spend another three or four more months verifying the code. CSEE Transport sought a more advanced and automated validation technique to ensure dependable operation of its software.

THE SOLUTION

CSEE Transport used PolySpace Client for Ada and PolySpace Server for Ada to identify run-time errors, including access to non-initialized variables, divisions by zero, and out-of-bounds array access.

THE CHALLENGE

To automatically identify run-time errors in security software for high-speed rail software

THE SOLUTION

Use PolySpace tools to automatically analyze 15,000 lines of Ada code

THE RESULTS

- 15,000 lines of code verified in hours instead of months
- More engineer time devoted to enhancing security
- Hidden defects uncovered

Using PolySpace to verify their software without executing it, CSEE Transport developers located errors that were undetectable by classical verification. These errors included concurrent access by parallel tasks to shared variables.

The CSEE Transport development team used PolySpace at each step in the software development process to validate individual modules before final integration.

THE RESULTS

■ **15,000 lines of code verified in hours instead of months.** CSEE engineers used PolySpace to analyze 15,000 lines of Ada code in just a few hours. In the past, verification of the system – including rereading source code and security analyses – took three or four months.

■ **More engineer time devoted to enhancing security.** By automating lengthy, difficult verification tasks, PolySpace reduced the workload for the CSEE Transport security specialists, enabling them to focus on more complex security problems that cannot be handled automatically.

■ **Hidden defects uncovered.** “PolySpace identified errors that can arise when parallel tasks access shared variables concurrently. These kinds of errors were undetectable when CSEE Transport developers used conventional verification techniques.

To learn more about CSEE Transport, visit
www.csee-transport.com

APPLICATION AREAS

- Rails, ships, and other transportation
- Control design
- Verification and validation

PRODUCTS USED

- PolySpace™ Client for Ada
- PolySpace™ Server for Ada

www.mathworks.com