PRQA Programming Research

Case Study

Lyon Metro – the implementation of a safety-related system under EN 50128 for their driverless trains

Viveris Technologies

Introduction

The deployment of driverless trains on the Lyon Metro, also known as MAGGALY (Métro Automatique à Grand Gabarit de l´Agglomération Lyonnaise), started on Line D in 1992. Line D has subsequently become the most popular line on the Lyon Metro, stretching 12.6 km / 8 mi, passing through 15 stations and carrying almost 80 million passengers every year.

The generic rationale for automating public transport systems is a combination of:

- improved operational efficiencies, for example by increasing the frequency of trains or the speed between stations
- reduced capital and/or operational costs
- improved safety and reduced risk

In a nutshell:

- Developed to EN 5012X, SIL 2
- Static analysis tool for safety-critical project: QA·C with MISRA C:2004
- 174000 lines of code
- 16 engineers and 2 technicians over 1800 days
  - Engineering
  - Design
  - Validation
  - Installation

The Project

Overall responsibility for the Lyon Metro lies with SYTRAL (Syndicat mixte des Transports pour le Rhône et l'Agglomération Lyonnaise), who has delegated the maintenance and operations of the Lyon public transport systems to Keolis. In 2009 PRQA's partner VIVERIS TECHNOLOGIES was awarded a public tender to modernize the platform safety system which detects if/when a passenger/object has fallen onto the track. This project had to comply to EN 5012X, and, more specifically the system had to meet SIL level 2.

The system consists of 768 parallel horizontal infrared beams, spaced 15cm/6in apart and passing above the track covering the length of each platform (see Figure 1).

When an infrared beam is broken – it is checked every 22.7 milliseconds - the relevant sensor is tripped and the system is designed to respond as follows (see Figure 2):

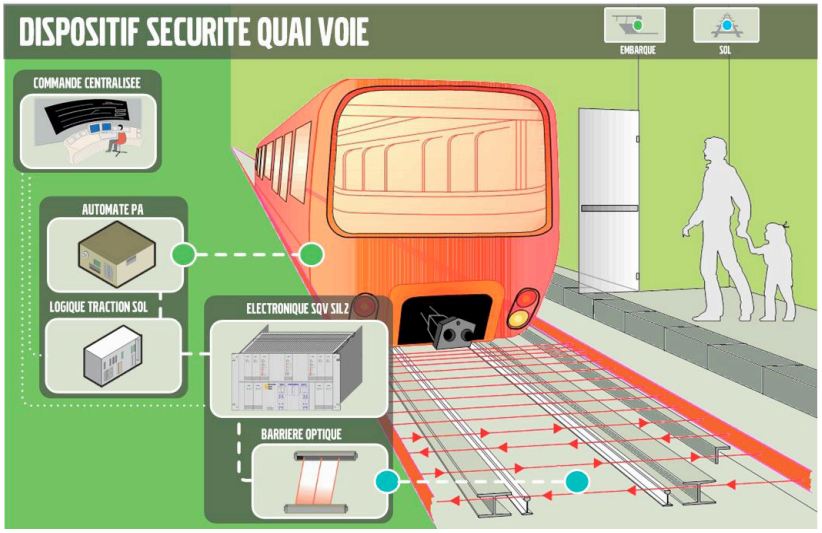


Figure 1

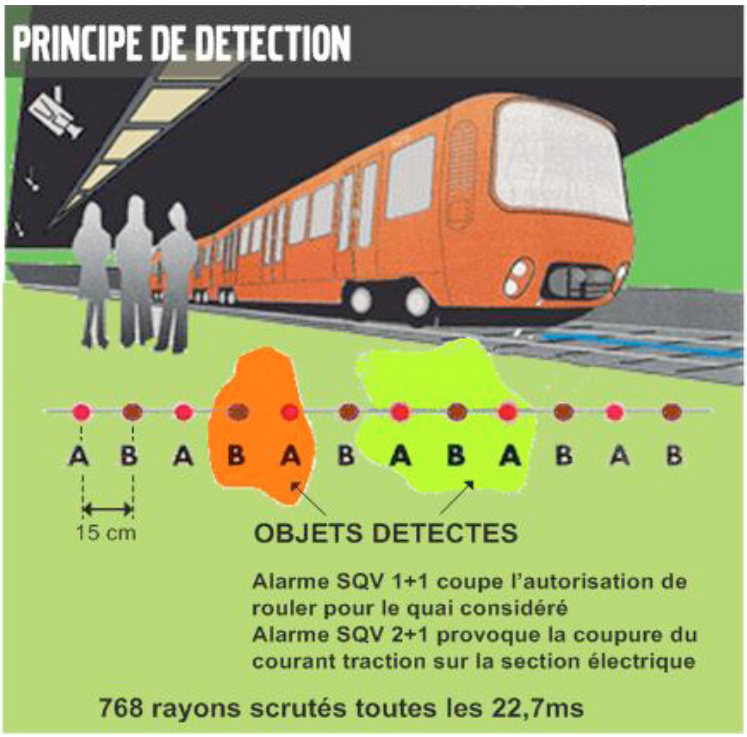


Figure 2

- **2 adjacent sensors tripped;** implies that a person or sizable object has fallen onto the track, and the system automatically stops the next train from reaching the platform.
- **2 + 1 sensors tripped;** implies a more serious incident and the system responds by stopping the next train entering the station as well as switching off the power to this section of track.
- **When sensors located beyond the edge of the platform are tripped;** this indicates an intrusion into the tunnel and brings the entire Line D to a complete stop. Power will not be reinstated until a visual check has been conducted by staff walking through the tunnel.

Note that cameras are also located above the track, providing additional information to help security staff to assess and deal appropriately with any incident.

The Implementation

In accordance with the SIL 2 requirements as defined under EN 50128, VIVERIS TECHNOLOGIES adopted the following three step process:

Step 1: system design
Step 2: development, testing and tuning
Step 3: installation, testing and commissioning

VIVERIS TECHNOLOGIES highlighted the fact that EN 50128 recommends the use of a coding standard (even for SIL 2), but does not specifically state which one. “MISRA was the obvious choice. Originally created by the automotive industry, it is one of the longest established and most respected standards, and has been widely adopted across multiple safety related markets”.

“Using a software verification tool that is already certified to EN 50128 is vital. This accelerated our development times, reduced our overall cost and mitigated our risk.”
Emmanuel Charbouillot,
Technical Manager at Viveris Rhône-Alpes

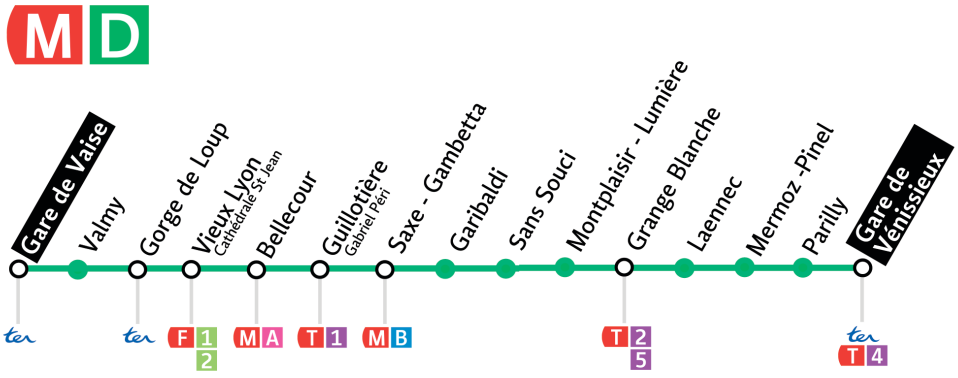
VIVERIS TECHNOLOGIES was equally keen to adopt best-in-class tools to verify the fact that their code is MISRA compliant. “The accuracy of QA·C was crucial”. Independent research* has shown that many other tools claim to cover MISRA but generate numerous false positives and false negatives. The former waste key resources as the developers need to invest time to eliminate this “noise”. The latter are more significant as false negatives are genuine MISRA non-compliances that a tool has failed to identify. Having these latent issues in the code can have serious consequences. Viveris also noted that “the cost and time required to test were significantly reduced as the test teams were receiving higher quality code”.

VIVERIS TECHNOLOGIES adopted the majority of MISRA C rules, across 174000 lines of code, and used the output from QA·C to provide objective/independent evidence of compliance to the auditor, including justifying, controlling and tracking legitimate deviations.

Prior to final commissioning, an audit was conducted on Viveris’ site to ensure that the development had complied fully with EN 5012X SIL2. The auditor specifically checked for the following:

- review of the entire project
- compliance – quality and organizational
- evidence that the MISRA rules have been enforced

The audit was successful and the rollout went ahead. The first deployment was installed in 2011 with all 15 stations operational by 2013.



* Independent Research on MISRA C Compliance Tools” available : http://www.programmingresearch.com/resources/white-papers/

The Future

VIVERIS TECHNOLOGIES also sees this as a test system to explore alternative uses of this core technology. In the near future, there are plans to extend this to cover train coupling/decoupling and in-tunnel evacuation situations.

About VIVERIS TECHNOLOGIES

VIVERIS TECHNOLOGIES, part of Viveris group, is today strongly established in R&D outsourcing and industrial IT markets.

Our offering covers the main areas below:

- Electronics
- Embedded systems
- Networks and Telecommunications
- Modeling
- Simulation

Our engineers are involved in:

- Aeronautics, Space, Defense
- Transportation
- Energy
- Medical

For more information, visit **www.viveris.com**

About PRQA | PROGRAMMING RESEARCH

Established in 1985, PRQA is recognized throughout the industry as a pioneer in static analysis, championing automated coding standard inspection and defect detection, delivering its expertise through industry-leading software inspection and standards enforcement technology.

PRQA's industry-leading tools, QA·C, QA·C++ and QA·Verify, offer the closest possible examination of C and C++ code. All contain powerful, proprietary parsing engines combined with deep accurate dataflow which deliver high fidelity language analysis and comprehension. They identify problems caused by language usage that is dangerous, overly complex, non-portable or difficult to maintain. Plus, they provide a mechanism for coding standard enforcement.
PRQA has corporate offices in UK, USA, India and Ireland, complemented by a worldwide distribution network. **www.programmingresearch.com**

Contact Us

For further information regarding PRQA products and consulting services, please contact PRQA via your local sales representative, or directly at: **info@programmingresearch.com**