PRQA Programming Research

ケーススタディ

リヨン市の地下鉄：列車の無人運転における EN 50128 準拠の機能安全に関するシステムの実装

Viveris Technologies

はじめに

MAGGALY（Métro Automatique à Grand Gabarit de l´Agglomération Lyonnaise）という名前でも知られているリヨン市の地下鉄における無人列車運転システムは、1992 年に D 線で運用が開始されました。その後、D 線はリヨン市の地下鉄で最も利用客の多い路線となりました。線路の全長は 12.6km、駅数は 15 駅、乗客数は年間約 8,000 万人に及びます。

公共の交通システムを自動化する一般的な理由としては、次のような要因が挙げられます。

- 運行における効率性の改善（例：運行本数の増加や運行速度の引き上げなど）
- 設備投資費や運用経費の削減
- 安全性の向上とリスクの低減

ツール展開の概要

- 適用規格：
  EN 5012X/SIL 2
- セーフティクリティカル関連のプロジェクトで使用した静的解析ツール：
  QA·C/MISRA C:2004
- コード行数：
  174,000 行
- プロジェクト規模
  （所要日数：1,800 日以上）：
  技術者 16 名と専門家 2 名
  - エンジニアリング
  - 設計
  - 検証
  - 導入

プロジェクトについて

リヨン市の地下鉄の全体的な責任を負うのが、ローヌ=リヨン都市圏輸送混合組合（SYTRAL： Syndicat mixte des Transports pour le Rhône et l'Agglomération Lyonnaise）です。同組合によって、リヨンの公共交通システムの運行管理は Keolis に委託されています。2009 年、PRQA のパートナー会社である Viveris Technologies は一般入札で契約を勝ち取り、利用客や物などが線路上に落ちたことを検知するプラットフォーム向け安全システム刷新プロジェクトに参加しました。このプロジェクトで開発する新システムは EN 5012X の SIL レベル 2 に準拠しなければなりませんでした。

新システムでは、各プラットフォームと同じ長さで、レール上に垂直になるように 15cm 間隔で 768 本の赤外線センサーを設置しました（図 1 を参照）。

赤外線が遮断されると（赤外線の動作確認は 22.7 ミリ秒で実施）、連動しているセンサーが起動し、システムが次のように動作するよう設計されています（図 2 を参照）。

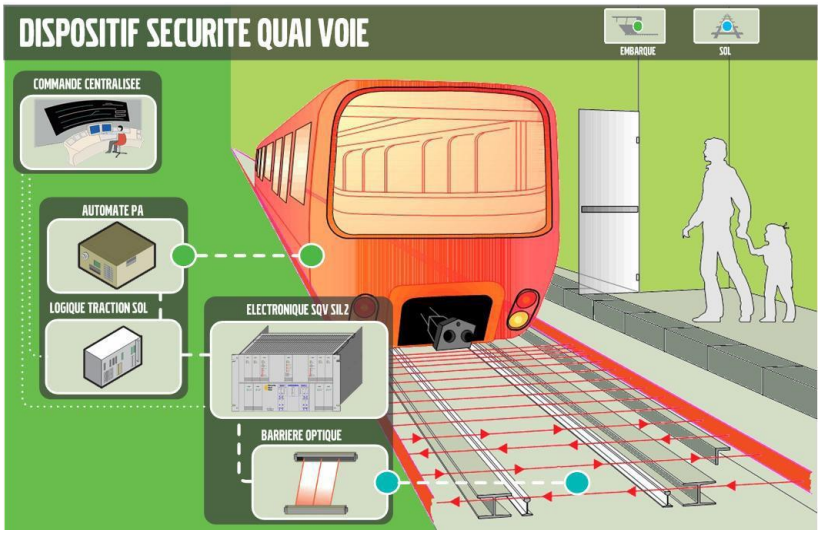


図 1

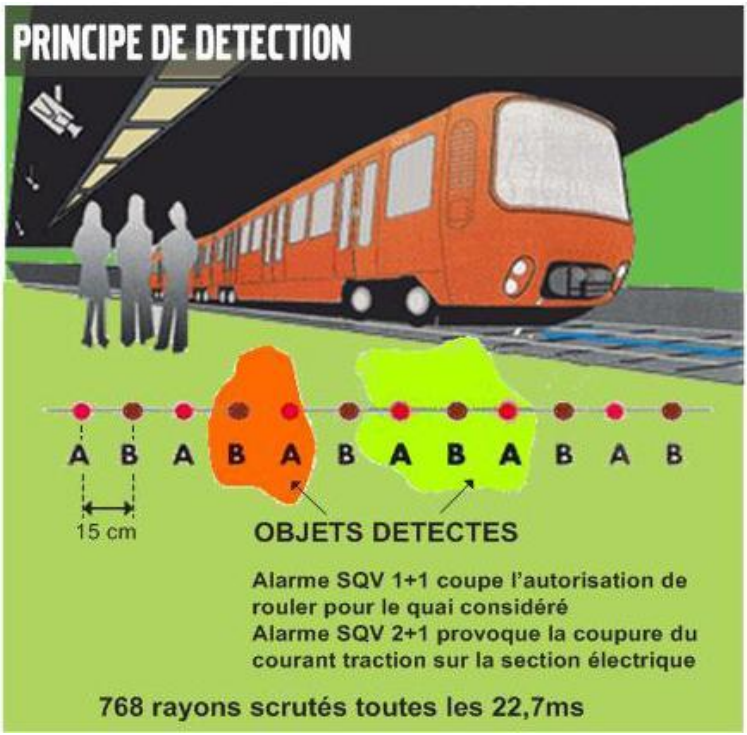


図 2

- **隣接する 2 つのセンサーが作動**： 人や、かなり大きな物が線路上に落ちたことを意味し、システムが駅に到着する前に次の列車を自動的に停止させます。
- **2+1 つのセンサーが作動**： より重大な事故を意味し、システムが駅に到着する前に次の列車を停止させ、さらに、この線路部分の電力供給も止めます。
- **プラットフォームの先に設置されたセンサーが作動**： 何者かによるトンネル内への侵入を意味し、D 線全体が完全に運行を停止します。駅員によるトンネル内の目視点検が完了するまで復電しません。

また、駅のスタッフがあらゆる状況に適切に対処できるように、線路を監視するためのカメラも設置されています。

実装について

EN 50128 で規定されている SIL 2 の要件に適合するために、Viveris Technologies は次の 3 つの手順に基いてシステム開発を行いました。

手順 1: システム設計
手順 2: 開発、テスト、調整
手順 3: 実環境での実装、テスト、試運転

EN 50128 ではコーディング規約（SIL 2 も含め）の使用を推奨しているが、厳密にどの規約を適用すべきかは述べられていない、という点を Viveris Technologies は強調しました。「自動車業界由来の規格ですが、最も長い歴史を持ち、高く評価されているガイドラインであること、さらに現在ではさまざまな安全性に関わる市場で幅広く採用されていることから、迷うことなく MISRA を選択しました」

「EN 50128 の認証を受けたソフトウェア検証ツールを活用することは必要不可欠でした。QA·C によって、開発時間の短縮、全体的な費用の削減、リスクの軽減を実現しました」

Emmanuel Charbouillot 氏
Viveris Rhône-Alpes のテクニカルマネージャ

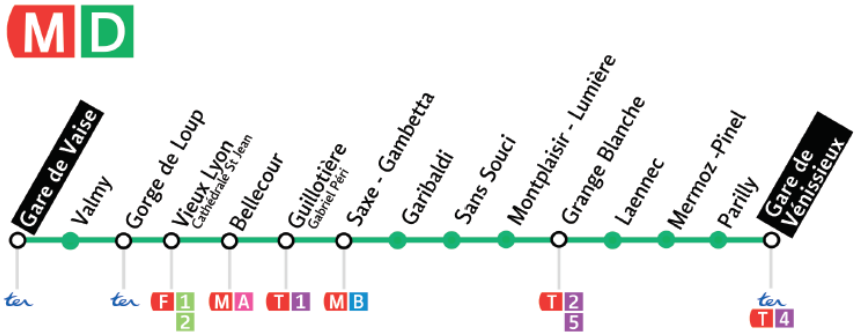
Viveris Technologiesは、自社で開発されたコードがMISRAに準拠していることを実証するために、最高峰のツールの導入にも熱心でした。「QA·Cの精確さが決定打となりました」。ある調査会社は「MISRAの準拠を謳うツールは数多くあるが、これらのツールでは大量のフォールスポジティブ(誤検出)やフォールスネガティブ(未検出)が発生する」との見解* を示しています。フォールスポジティブが発生すると、この「ノイズ」を除去するために開発者の時間が割かれ、重要なリソースが浪費されます。フォールスネガティブの場合、MISRAに準拠していないにも関わらずツールが検出し損ねている、という点でより深刻です。これらの問題がコード内に潜んでいることは、重大な問題を招きかねません。さらにViveris Technologiesは、「テストチームは品質の高いコードで検証を行えるので、テストに要する費用や時間も大幅に抑えることができました」とも述べています。

同社は MISRA C ルールの大多数を 174,000 行のコードに適用し、コンプライアンスの客観的かつ公平な証拠（逸脱の正当性を証明するデータや、それら逸脱の制御/追跡情報を含む）を監査員に提出するために、QA·C の出力を活用しました。

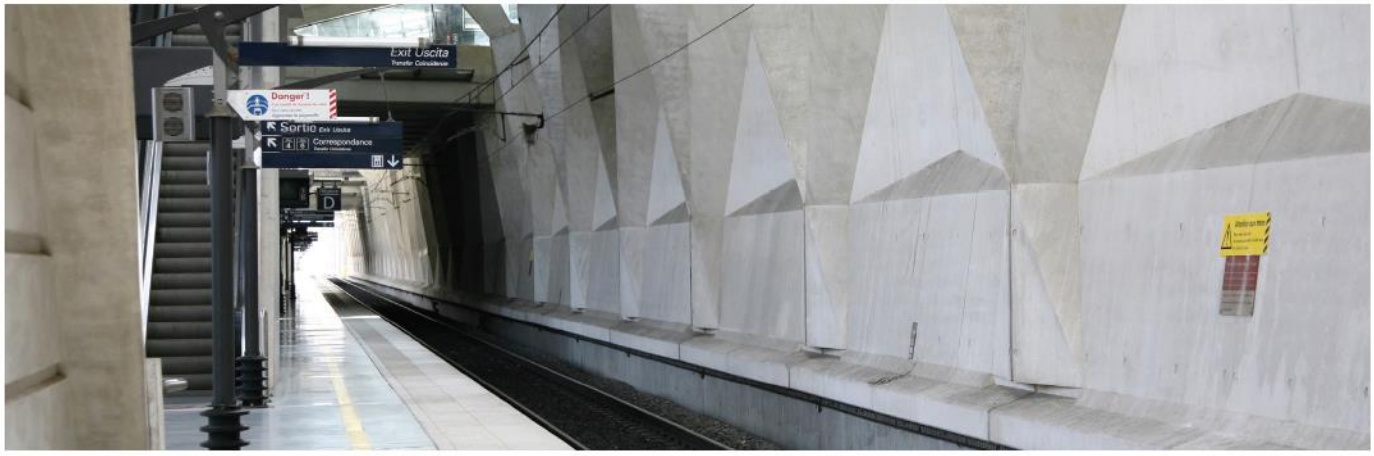
最終的な運行試験へ移行する前に、開発内容が EN 5012X SIL2 に完全に準拠していることを確認する目的で、Viveris 社内での監査が実施されました。監査員が行った具体的な検査内容は次のとおりです。

- プロジェクト全体のレビュー
- コンプライアンス: 品質と構成
- MISRA ルールへの適合を示す証拠

監査に見事合格し、新システムが展開されました。最初の導入は 2011 年に実施され、2013 年までに全 15 駅で実用化されました。



＊ MISRA C 向けコンプライアンス適合性チェックツールの独自調査の内容は、こちらを参照



今後の展望

Viveris Technologiesは、今回の地下鉄用安全システムで用いた技術を、他の用途にも転用することを検討しています。近い将来には、車両の連結/分離や、トンネル内での避難対策も視野に、この技術を拡張する計画が立ち上がっています。

Viveris Technologies について

Viveris グループの 1 企業である Viveris Technologies は、R&D アウトソーシングおよび IT 産業市場において、確固たる地位を確立しています。

主な事業分野は、以下のとおりです。

- 電子技術
- 組込みシステム
- ネットワークと電気通信
- モデリング
- シミュレーション

また、同社の技術者は以下の分野で活躍しています。

- 航空学/宇宙/防衛
- 輸送
- エネルギー
- 医療

詳しくは、**www.viveris.com** をご覧ください。

PRQA | PROGRAMMING RESEARCH について

1985 年に設立した PRQA は、業界内ではコーディング規約の自動検査や欠陥の検出を支援する、静的解析ツールの先駆者として認められています。また、ソフトウェアにおける標準規格などへの適合性を評価する、業界最高レベルのテクノロジを通して、その専門的な技術を提供しています。

PRQA の業界トップクラスのツールである QA·C、QA·C++、QA·Verify は、極めて厳密に C/C++のコードを検査します。すべてのツールには、強力な独自の構文解析エンジンが実装されており、複雑かつ的確なデータフローを併用して、非常に忠実な言語解析とその解析結果を提供します。また、危険、複雑すぎる、移植性がない、または維持管理の難しいコードの記述によって生じる問題を特定することが可能です。これらにくわえて、コーディングルールに準拠するためのメカニズムも用意されています。

PRQA は、イギリス、アメリカ、インド、アイルランドに拠点を展開し、世界各国に販売網を築いています。

お問い合わせ

PRQA の製品やサービスに関するご意見ご要望は、東陽テクニカのソフトウェア・ソリューションまでお寄せください。

商標について