How to reduce qualification time for new safety automated systems on rail infrastructure

Claire Guegan[1], Franck Corbier[2]

1: RATP, 40 bis, rue Roger Salengro - 94724 Fontenay-sous-Bois Cedex
2: GEENSOFT, 3, Allée d'Auteuil - 54500 Vandoeuvre-les-Nancy

Abstract: With 10 million passengers transported every day, RATP has been investing in transport modernisation to cope with the continuous growth of traffic, to offer an up-to-date response to passenger expectations, and to optimize economical and environmental performances.

Figure 1 : The metro of Paris, more than 110 years of history

As part of the Paris Metro modernisation program, RATP chose to develop a novel metro management system called OURAGAN.

Leveraging communication based train control, OURAGAN allows traffic operators to reduce the headway between two trains in complete safety, as more trains are available for passengers during peak hours. Such systems become increasingly complex as well as difficult to integrate and qualify.

This paper will present specific tools and methods used to dramatically reduce time and costs devoted to on-site tests.

Keywords: Signalling, Transportation, Model based Design, Progressive Integration, Validation, Safety, Quality, Qualification, EN-50128.

1. Introduction

The major difficulty resides in the connection and integration of safety systems (electronic control units distributed on network) with original and existing safety signalling systems, that gives different response times and input data.

Traditional tests are usually performed at night when the traffic is closed. To be completed, on-site tests require a lot of time (around 1000 nights) and resources (test engineers but also drivers and traffic operators).

RATP introduced *exchangeability* into the OURAGAN project, turning it into *Generic OURAGAN project*. This strategy offers flexibility, guarantees system supply from multiple sources and provides cost efficiency.

It became essential then to focus on methods and tools based on new "virtualisation" concepts which apply to specification, validation and training. In order to qualify the OURAGAN system, RATP launched the "System Integration & Qualification Bench" (BIQS) project. This project implements specific methods and tools that scale to the complexity level of systems such as OURAGAN, making system integration and qualification phases significantly more effective.

2. OURAGAN Hardware Architecture

Major issues are to interface the OURAGAN system with existing instrumentation (historical knowledge) of the line (campaign, signalling), the local control station and the central exploitation control of the line.

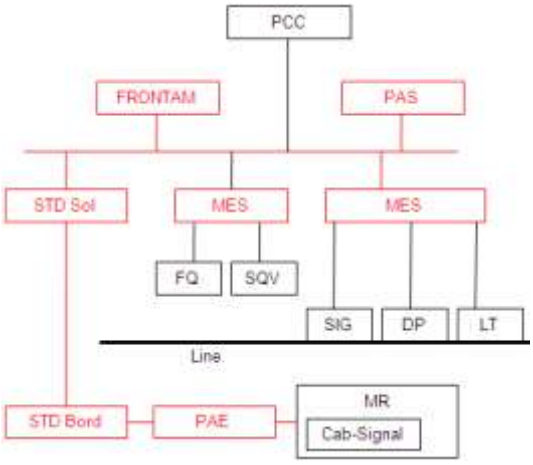

Figure 2: OURAGAN in its environment

OURAGAN is composed of a distributed architecture with various computers, interconnected through a communication system: a dedicated field network and a radio network with train.

OURAGAN consists of five modules:

- PAE: Autopilot embedded on the train (one Electronic Computer Unit by train),
- MES: Remote I/O Module interfaced with equipments of the line (rails, signals, switches),

- PAS: Autopilot on the ground (each one manage one part of the physical line),
- FRONTAM : Interface between OURAGAN and the central control and exploitation of the line,
- STD: Intelligent Communication System management.

3. Integration and Qualification needs

Main objectives of the BIQS bench are:

- to improve integration phases, set up and validation of a new line using tests management on the laboratory bench,
- to monitor the OURAGAN system during its life cycle (operation and maintenance activities) and to support investigations and assist diagnosis,
- to test and validate future evolutions and changes of the system,
- to serve as a reference for exchangeability.

Objectives and tasks of the system qualification bench are based on the following concepts:

- Ability to simulate an entire line with real time constraints and representative behaviour,
- Ability to integrate and co-simulate different models (train, line, traffic, signalling, safety rules, autopilot…),
- Ability to swap a target model with the real target without heavy reconfiguration,
- Ability to emulate the data transmission system,
- Ability to obtains degraded modes of system functions by fault insertion,
- Ability to place the test cases in automatic mode as well as in interactive mode,
- Capacity for flexibility and extension of the configuration line,
- Ability to provide HMIs to facilitate the analysis,
- Ability to re-play incidents recorded on the line.

All these concepts put together represent a major innovation in the context of RATP projects.

Because OURAGAN markets are allotted, the manufacturers which support implementation of "bundles" have a fragmented view of the overall system and the interfaces shall only be liable for their services. Final integration of system components remains a matter of on-site testing, on the basis of tests of actual situation on the line.

Moreover, realization of such an integration and qualification bench requires pooling knowledge from different actors, who are either dedicated to control systems, either experts of simulation, either managers able to cope with complex organization and systems.

To limit the risks of developing such a system, RATP has decided to start with a first step called “demonstrator”, intended to confirm feasibility of main concepts involved. This demonstration is based on the implementation of recognized industrial know-how, in the field of system simulation and qualification benches development.

Consequently, the main requirements for this bench have been classified into three categories:

- Support for integration and validation
- Support for systems maintenance
- Qualification of a new supplier, in compliance with OURAGAN *exchangeability* requirement

3.1. Support for integration and validation

Objective is to validate the system off-line, to reduce on-site qualification time and avoid operation disruptions.

3.2. Support for systems maintenance

One primary purpose is to maintain the system in operation and to detect root causes of anomalies occurring in exploitation, using registered data (black box). The idea is to strip incidents, to analyze registered events and to visualize/check them with friendly HMIs and tools. Such services can automatically create scenarios (tests vectors) to replay real-time situations on the bench.

3.3. Qualification of a new supplier, in compliance with OURAGAN *exchangeability* requirements

The BIQS bench helps qualify the target provided by a new manufacturer, before adding it in to the reference list of compliant OURAGAN equipments. This target will undergo standard test sets and both final and expected results should match for compliance: standard test procedures are applied to new targets and test results are automatically compared with the expected results.

4. BIQS Hardware Architecture

To meet the needs of integration and validation, the BIQS bench qualification system needs to simulate the complete OURAGAN system environment, to host the electronic control units of the entire system and allow test cases to be run.

This complete environment, including signalling, line, and trains, as well as all OURAGAN safety and control functions have been modelled and simulated using ControlBuild. Automatic test scripts (traffic and failure modes) have been applied on the line model, providing fast and comprehensive analysis results.

A uniqueness of the BIQS bench lies in the fact that the real ECUs developed to meet the OURAGAN system can be, at will, either *connected to* or *simulated on* the bench. In addition, a device created by Vendor A may be replaced by another ECU made by Supplier B, alternatively by a simulation model.

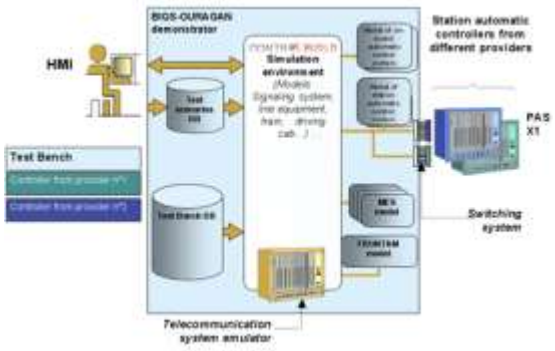

Figure 3: System Integration and Qualification Bench

5. Software Architecture

RATP has a test base located on the 8th Metro line in Paris at the station "Porte de Charenton".

The goal of this first implementation is to create a virtual model of the line, which, from the electronic equipments perspective, will behave exactly like the real one.

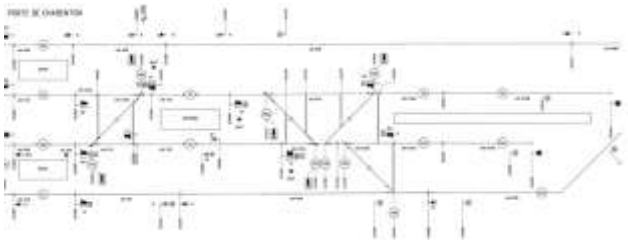

Figure 4: Map of the test line "Porte de Charenton"

The qualification bench is composed of simulation models (the physical environment of the line, the rolling stock (trains) and controllers that are not present), test scenarios and the communication between all equipments (interface configuration of I/Os and network communication)

5.1. Simulation Models

Models are replacing the environment but also the targets under test themselves (because these are not always available in the test platform).

All these models are characterized by:

- interfaces that can be connected to I/O or data networks to communicate with other models,
- state variables representing the behaviour of the model or its parameters (movement time, platform length, time of opening doors, required speed ...),
- simple or complex transfer functions depending of the expected behaviour,
- specific parameters used to modify the normal behaviour of the model (creation of mechanical, electrical or communication faults).

The BIQS bench integrates different types of models:

- Environment (line, signalling, rolling stock and local control board models)
- Electronic equipment models (automatic pilots)

5.1.1. The Environment models

These models simulate the environment of autopilots to be qualified. They represent the behaviour of the line, signalling, power distribution, interfaces of local or centralized control room and the train (cab, traction, doors, localisation sensors and also the virtual driver).

Model of the line: all objects that guide the movement of the train are included in the line model. The line model contains tracks, switches, signals and detectors, platform, tunnels ...). Each object refers to a behaviour model. Each object has a graphic animation and is set in the 3 axes dimension. Geensoft has developed software that *automatically* builds up the ControlBuild model line from a database containing the geographic parameters of all objects on the line.

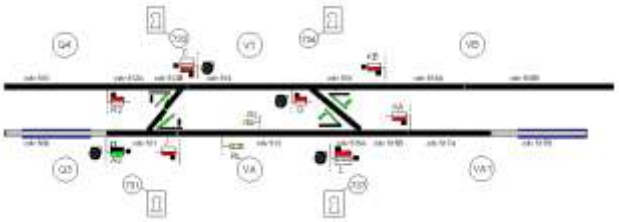

Figure 5: Physical line with traffic

Signalling model: The current Paris Metro signalling system that ensures safety control is primarily done in electrical hardware. This system will have to coexist with the new electronic controlled system. It is therefore necessary, for the qualification bench, to develop the model of the signalling hardware.

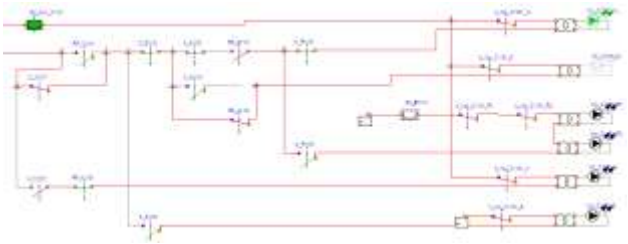

Figure 6: Signalling schemes

The original electrical schematics are printed on paper. They have been seized manually in the ControlBuild modelling tool. A comprehensive code review verification phase has been implemented to compare the original diagram with the model. The final acceptance phase has been performed by Safety engineers who were able to validate the model using simulation and test.

Local Station Control model: when the line is disconnected from the Central Control System, the RATP agents have a local traffic control for managing trains within the station. The Local Station Control consists of a board witch displays signals, switch positions and occupied tracks. A panel allows the agent to manage the station's equipments to build expected routes.

A model of the Local Station Control of the “Porte de Charenton” test platform was developed in ControlBuild and integrated in the qualification bench.

Figure 7: Visualization panel in station

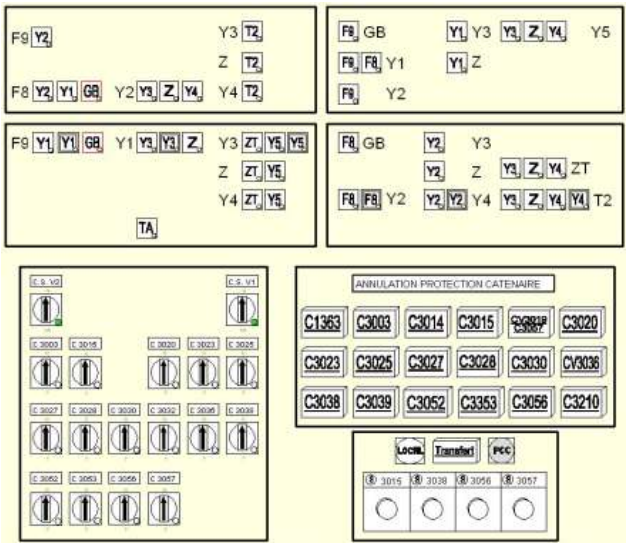

Figure 8: Control panel in station

Rolling Stock model: For our needs, the model of the train consists of the integration of software modules including the driver cab, a simplified rolling stock (doors, rail lines, power distribution ... pantograph) and the traction. The dynamic characteristics of the traction model are quite close to those of a real train, to obtain a representative behaviour along the line.

The rolling stock model is simplified in order to deliver the necessary interfaces to drive the train model “by a conductor”. The panel driving cab has been generalized to enable the same driving modes whatever rolling stock types can be.

Figure 9: Panel driving cab

Interaction between the train and the line: ControlBuild has a function to move a train in a three-dimensional space without any programming. So the train can move along the railway tracks, detect the position of the switch track, respond to sensors and capture the power of the catenaries with a pantograph... This module is interfaced with the traction model to calculate the speed of the train, based on requested acceleration.

5.1.2. Autopilot models

Real electronic processing units (automatic pilots) can either be present or absent on the test bench. Hence, it has been necessary to develop models (virtual clones) that are able to simulate the functions supported by the non present target. These models can be dynamically enabled or disabled depending on the presence of the real equipment.

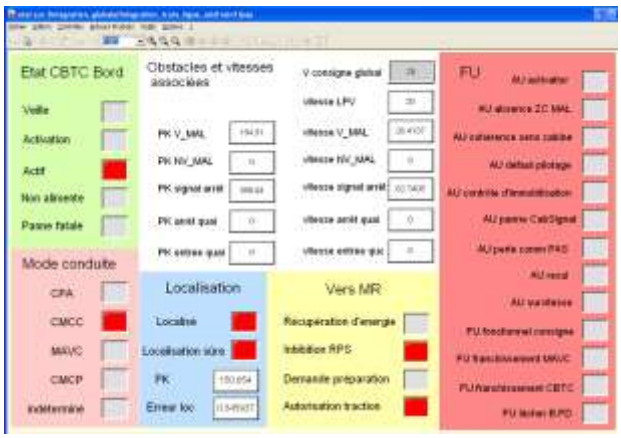

Figure 10: Display of the autopilot interfaces states

Autopilot functions required to roll out tests on the “Porte de Charenton” station have been developed using virtual electronic equipments:

- Reconfigure a disabled area
- CBTC activation
- Compensate for faulty tracks circuit
- Help for automatic cancellation of a route
- Help for emergency cancellation of a route
- Secure approach locking
- Realise and free overrun locking
- Adhere to signalling indications
- Set direction
- Set train protection
- Detect fault of track circuit
- Handle passengers protection
- Control Safety on line
- Authorize regeneration of energy when braking
- Forbid driving modes
- Authorize entry into a station
- Supervise for operating assistance

5.2. Test scripts

The qualification bench can be operated manually or in automated modes. In manual mode, the GUI for the simulation models (line, signalling, cabs, rolling stock ...) enable testers to drive the trains along the line (route development), to verify the correct operation of the real (and simulated) equipment and create failures to validate the safety functions and faulty modes.

ControlBuild allows test engineers to describe test scripts that act on the models, so as to trigger actions related to nominal operation modes (eg locate a train, wake up the train, change the driving modes, accelerate or brake) or to cause abnormal situations (e.g., forcing a failure on a part of the system or on an equipment). Test cases are sequences of operations providing events on inputs and measurements on outputs. These procedures can also be automatically executed on the qualification test bench.

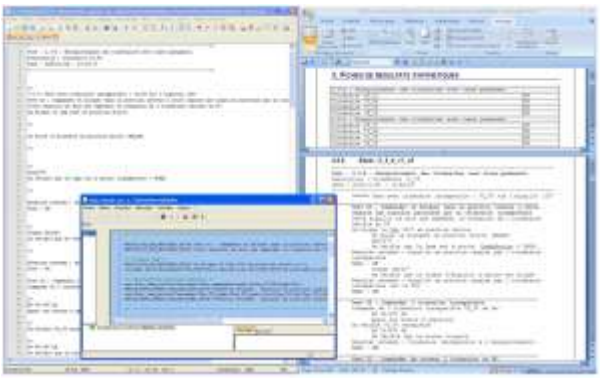

Figure 11: Test scripts editor and generated test reports

The main test script loads the initial context of the current test (fixed state of simulated equipments and environment) and then sequentially executes all code instructions according to the desired test. At the same time, other scenarios may simulate failures, trigger events (expected or not) and force the state of some equipment models.

Test scripts provide code instructions for the configuration of inputs/outputs and communications interfaces between the test bench and the real hardware ECUs to qualify. These instructions allow test engineers to cause faults on all interfaces and communications.

5.3. Physical interfaces of the bench

The objective of the test bench is to qualify hardware targets before their integration on the site (or inside the train). For this purpose, it is necessary to connect the targets to the bench; the BIQS test bench provides inputs/outputs and communication subsystems.

5.3.1. Inputs/outputs subsystem

The acquisition subsystem is expected to stimulate the inputs of physical targets, to measure the outputs value of the equipments, additionally to supply real targets with power.

For each signal, the subsystem ensures adaptation of electrical channels, digitization of analog sensor levels and time stamping of events. The BIQS test bench hardware subsystem is also able to support standard or specific communication networks.

A configuration editor allows customization of inputs/outputs cards and communication protocols on the qualification bench.

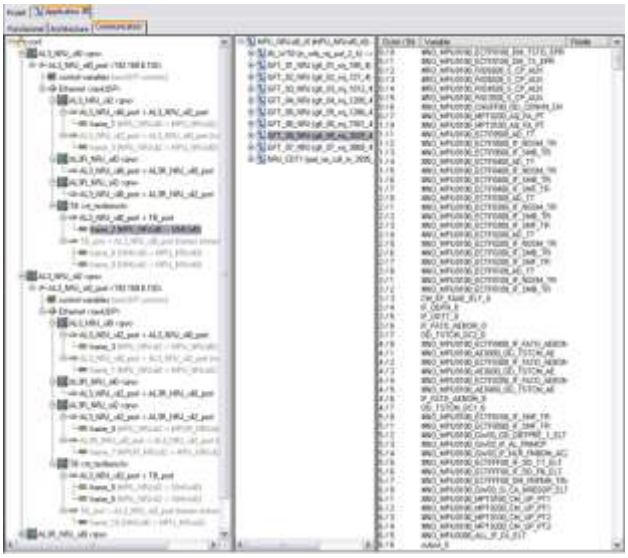

Figure 12: I/O and networks configuration

5.3.2. Communication subsystem

In the OURAGAN system, the communication medium is based on UDP. All exchanges are managed by an electronic device called STD (Data Transmission System). Its main function is to route messages between the equipments (physical targets or simulated target) of the OURAGAN system.

The behavioural model of this communication equipment has been developed with ControlBuild. It has specific modules to store the exchanged frames and disrupt the traffic data in real time.

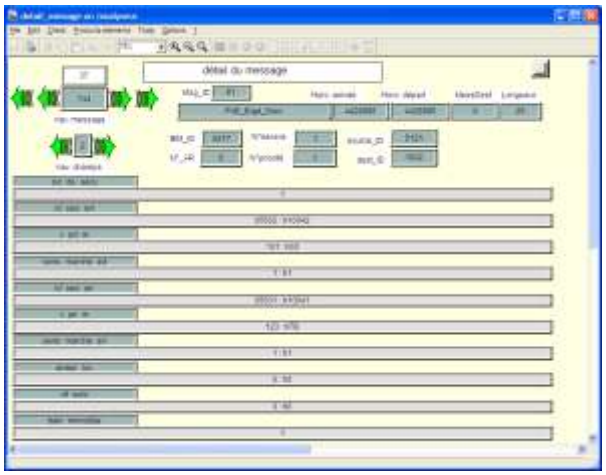

Figure 13: Spy, Data login and Communication monitoring

The simulation of malfunctions of the communication system allows test and safety engineers to verify the capability of real equipments, detect faulty behaviours, and take the right decision (continue, stop, secures, alert…).

7. Conclusion

This *System Integration and Qualification Bench* project demonstrates the key advantages of using proven simulation technologies to address safety automation issues. Key factors of success reside in the versatility of the simulation tool used, i.e. ControlBuild, particularly well suited for transportation sectors and in the flexibility of the methods and process used (from Model to HIL).

Gains achieved by implementing this solution measure up to the costs of downtime and operation of the real infrastructure when system qualification tests are performed on site.

"One day of tests with simulation represents up to ten nights of onsite tests!"

Beyond this novel "test bench" adoption, RATP will address other activities pertaining to the system engineering process.

This Model Based Testing technology seems to be promising, in terms of technical purposes, for validation of specifications before system development.

The high-level languages provided by ControlBuild allows the designer to easily describe the different environment models of the line (campaign, signalling, power distribution), to reuse rolling stock models and to prototype new automation requirements (safety control or not). These use cases can be validated by the different project stakeholders (engineering, safety department, traffic operation engineers…).

Since the model is representative of the system, the integration and qualification bench may be a support for investigations once the system is in use. All events detected in real operation can be inserted in the test bench for analysis.

The model could also be used to train the RATP workers on how to manage the traffic though the station when the communication with the automatic or central control room is off. It would then be possible to create situations, events and incidents that should never happen in the real life: the objective is to increase officer's awareness of incidents that may occur and to give them the ability to take the right decisions in stressful situations.

8. Glossary

BDD	Data Base
CV	Canton Virtuel
DP	Détecteur Ponctuel de passage
ECU	Electronic Control Unit
ERTS	Embedded Real Time System
FQ	Façade de Quai
I/O	Inputs / Outputs
HIL	Hardware In the Loop
MAL	Movement Authority Limit
MES	Remote I/O Module
MMI	Men Machine Interface
MR	Rolling Stock
PAE	AutoPilot, embedded in the rolling stock
PAS	AutoPilot along the line
PCC	Poste de Commande Centralisé
PMI	Poste de Manœuvre Informatisé
RATP	Régie Autonome de Transport Parisien
SQV	Surveillance Quai Voie
STD	Data Transmission System