INNOVATION & RESEARCH

BURIER Marc 02/09/2010

Marc BURIER
RATP

Systems Design
Railway Transportation Systems
Engineering Department

marc.burier@ratp.fr
Phone : 01 58 76 60 87

BARFID Project

Train detection safeguard based on Radio Frequency Identification (RFID) technology

- Basic needs description
- Legacy system
- Technological constraints
- Proposed principle
- Project phases
- State-of-the-art RFID technology
- Context of use
- Line 1 demonstration test bench

Description of the basic needs

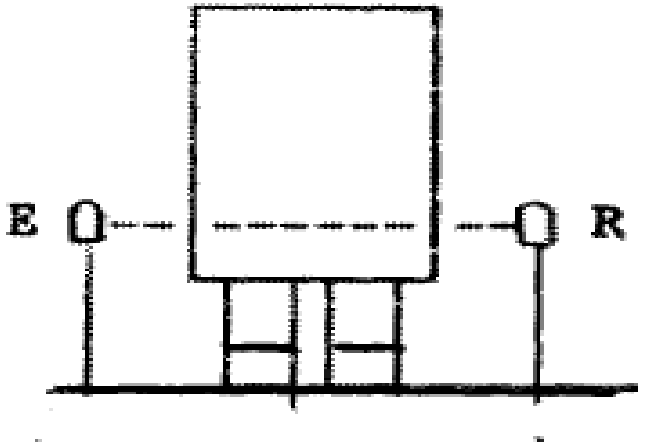
- 1 : Safeguard against driving errors
- 2 : Detect entry into specific areas
- 3 : Ensure that a train inside a maintenance area is at standstill

Legacy system: infrared detectors

Components of the infrared detectors

The detection system consists of:

- ✓ Emission component
- ✓ Detection component
- ✓ Support of the emission component
- ✓ Support of the detection component



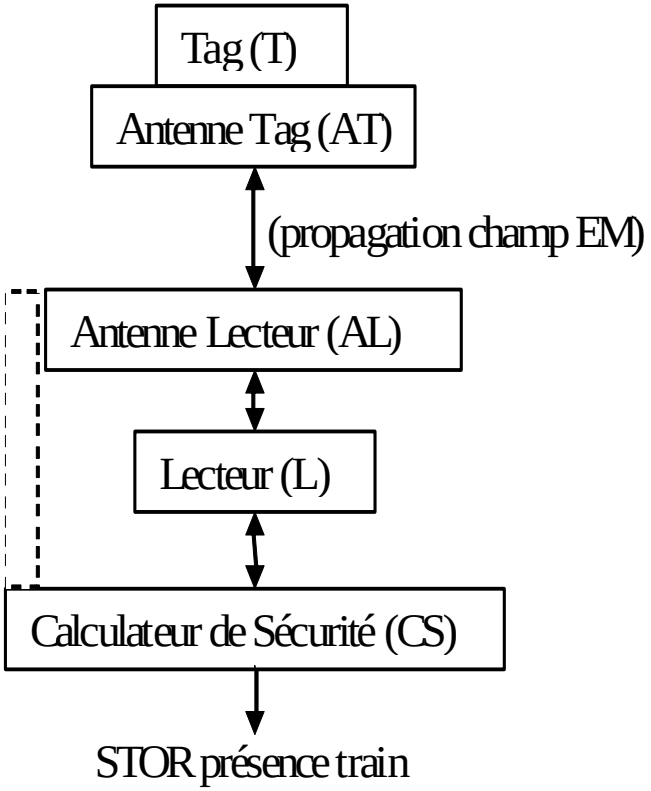
Line 14 example: redundant detection

Constraints imposed by the technology used

- Detectors require a large concrete base to ensure long-term high-level stability, which results in high costs and feasibility risks
- Optical technology requires regular and frequent cleaning and preventive maintenance actions.

Detection principle

- The design principle of the new RFID system is negative detection:
  - One or several fixed tags are located at the safe limit
  - The tags are read continuously by a safety processor
  - The presence of a train at the safe limit prevents the reading of the tags
  - The processor then delivers a safety-related STOR output that signifies that there is a train at the safe limit



An innovative project

Innovation in the BARFID project comes from the association of two things:

- An innovative use of the RFID technology
- Application of RAMS requirements to a system based on RFID technology

RFID technology is typically used for object detection and identification based on the reading of tags that are attached onto the objects to be identified. In the BARFID project, tags are instead embedded at particular sites (e.g. safe limits), read continuously, and it is the absence of reading caused by the presence of a train that provides the information that there is a train and thus constitutes detection.

RAMS constraints are normally not a concern in the usual application of RFID technology: if detection does not occur, a second opportunity is usually always possible. This possibility, however, does not exist in the case of train detection: not detecting a train is simply not an option.

Using RFID technology for safety-related systems

- Up until now, RFID technology has never been used in a safety-critical system
- Safety-critical systems are systems where a failure or a fault can have serious consequences on the life and safety of people, on property or on the environment

Project phases

- **Phase 1**

  - Analysis of basic needs and legacy system
  - RFID technology: looking for the available products adapted to the application and checking current state of the art
  - Design and feasibility studies (several alternatives are compared)
  - Dimensioning tests performed on site (inside a tunnel) with standard RFID products. These tests, carried out at RATP's dedicated site, have already delivered encouraging indications as to the feasibility of the RFID part (using UHF EPC gen2)
  - Initial hazard analysis: identification of safety-critical aspects. This analysis has to be carried out very early in the design phase to identify the necessary safeguard principles and thus ensure feasibility of any future industrial safety-critical product
  - Specification and realisation of a demonstration test bench for extensive tract tests and validation of the design solutions (site at Château de Vincennes station on Line 1).

  - Moving on to Phase 2 is dependent on the results of Phase 1

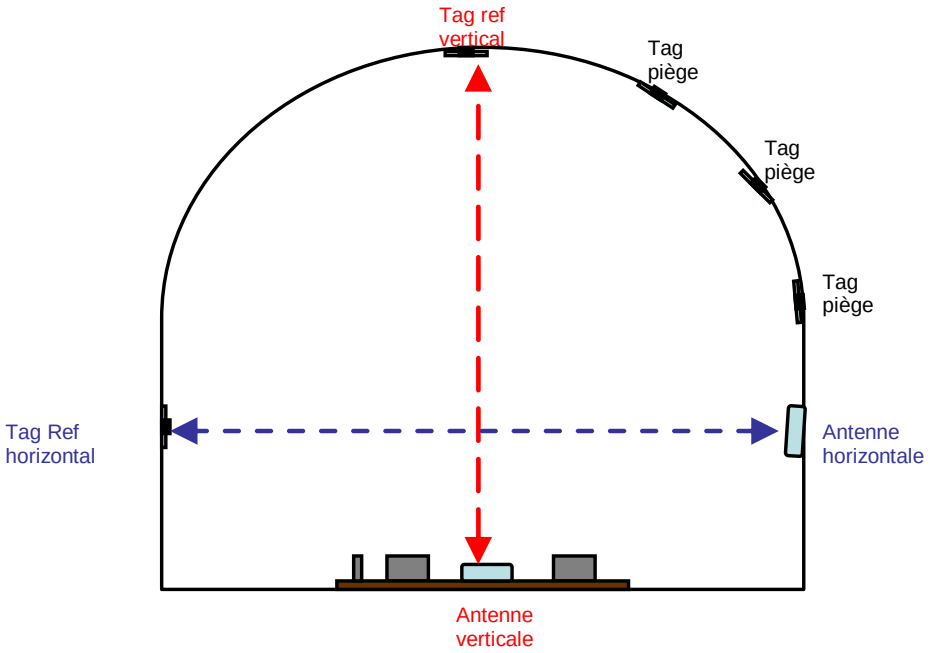
- **Phase 2**

  - Safety studies
  - Industrialisation of the product
  - Business Plan

State of the art

Dimensioning tests

- RFID UHF (the red line)
  - Measure of the maximum distance with effective detector antennae/tag communication depending on reader power
  - Test of several antennae locations (low, trackside) and tags (high, trackside); tags are used either as detection reference (negative logic relying on the absence of reading) or as traps (reading occurs when there is a train)
  - Assessment of the possible interference caused by secondary paths, most notably between two adjacent cars of the same train
- RFID HF (the blue line)
  - Test of an antennae and measure of the maximum antennae/ train distance (on the principle of magnetic detuning).



Implementation context

Specific provisions for on site implementation

Provisions must ensure minimising the influence of the following factors:

- ✓ Tunnel height
- ✓ Several safe limits in close proximity of each other
- ✓ Environmental conditions
  1. Sun
  2. Dew, water condensation
  3. Water projections
  4. Hail projections
- ✓ Indoor/outdoor installation
- ✓ Dust projections
- ✓ Electrical arcs (sustained or not)
- ✓ Detergents used for washing and cleaning vehicles

Formal methods applied to RAMS specifications

Formal methods

Formal methods provide a mathematical model for rigorously defining the characteristics of the functioning system. They apply at all stages of development, from specifications to implementation

Reliability and safety

- The objective is to ensure with a given level of confidence that any unsafe behaviour of the system or subsystem is made impossible. This guarantee on behaviour requires that the control of the functioning of the system or subsystem be rigorous and be seen to be rigorous.
- It is highly recommended to apply a formal method from the very beginning of the development of the system, i.e. the specifications stage, and at the safety specifications stage for systems with high SILs (SIL4 according to EN 61508, and SIL3 and SIL4 according to EN 50128).
- A formal method ensures a structured specification phase so that safety requirements are precise, univocal, verifiable, testable, maintainable, and devoid of any ambiguous terminology or description that could mislead the users of the specifications during the development cycle

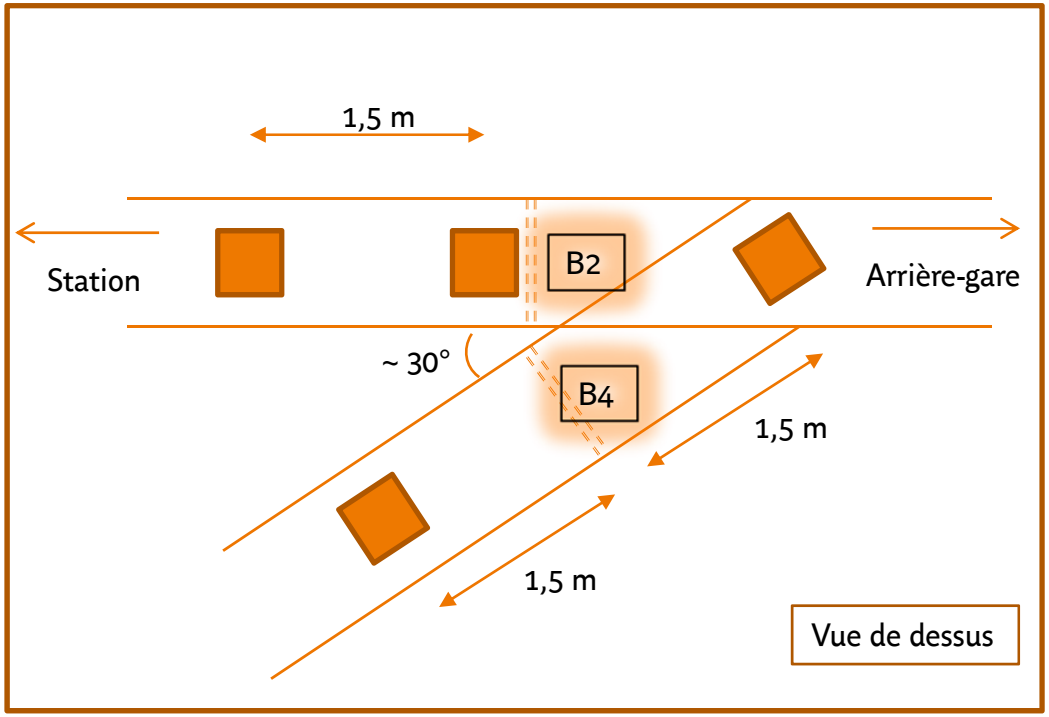
En pratique

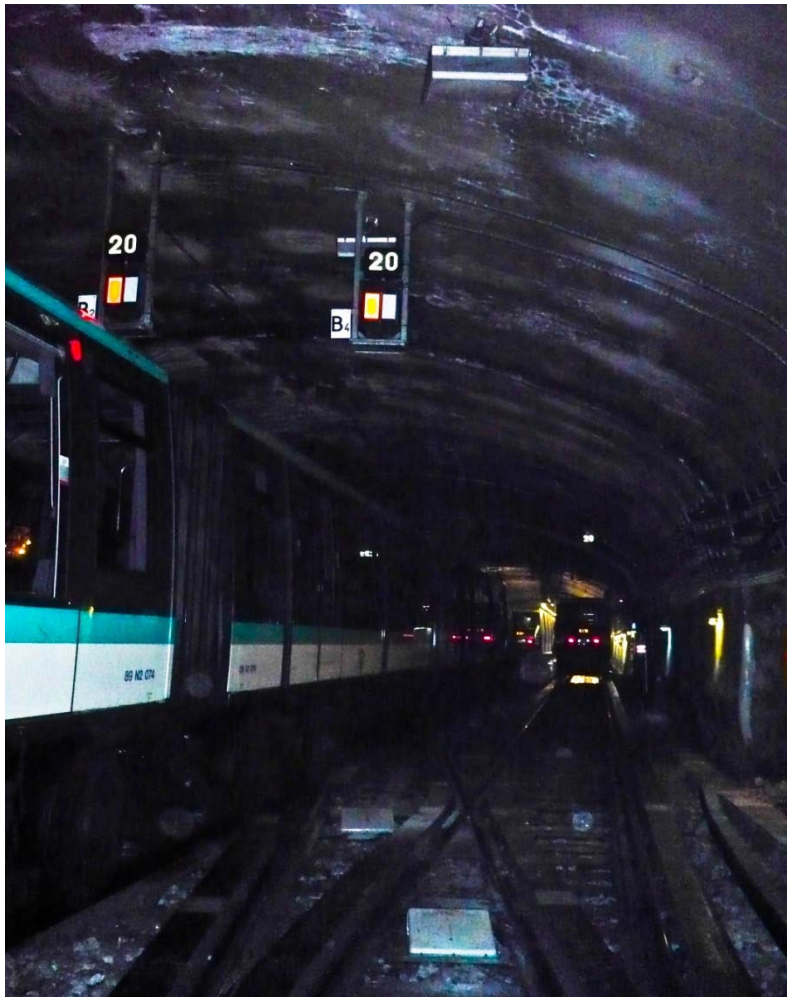
- **Usually, constraints may be:**
  - Architecture of the system: prevent common-mode failures
  - Documentation management: all components must be documented, in particular their interfaces with other components
  - Project traceability: the system must comply with each specification, including at the implementation stage and intermediary specification (which also have to be replied to). There must be a complete traceability between functional specifications and the implementation of the system
  - Restriction on hazardous practice: some software development techniques (e.g. dynamic memory allocation, recursive procedures and functions) are potential hazards and must therefore be either prohibited altogether or justified by imperative reasons
  - Testing: software must be tested for a large number of configurations that cover all the possible states of the system and as many as possible of the functioning path of the software
  - Use of development and validation tools: they must be safe themselves
  - Systems that are highly critical in terms of safety are generally subject to the certification of safety authorities who control that the system complies with safety standard requirements and deliver an approval
- **The use of formal methods may be encouraged, or even imposed**

Démonstrateur

- Line 1 opportunity study
  - Need to install safe limits at two signals (B2 and B4) at Château de Vincennes station.
  - No possibility of installing IR detectors for lack of available room.

Besoins métro L1






89 N2 030


20
20

Thank you for your attention

Any questions?