Special talk - Railway Track - Seville, Spain - October 21-23, 2015

Industrial needs concerning the safety analysis of a French implementation of ERTMS

Philippe BON, Simon COLLART-DUTILLEUL

IFSTTAR/ESTAS, 20 rue Elisée Reclus, Villeneuve D'Ascq

The study is based on an industrial expression pointing ausual way of performing a safety analysis: one consults the national railway accident database in order to evaluate the defense capacity of the system against scenarios of real past accidents.

This first analysis can be complemented by considering the quasi- accident scenarios. The data corresponding to this second step are critical because they correspond to industrial data which are not public.

A first result of this study is the identification of a class of accident. The main argument is that the similarities of two accidents or quasi accident allow defining some critical elements of a typical class of accidents. A case study of an analysis of the accident that occurred in "St Romaine en Giers" is proposed. The corresponding documentation may be found in [1]

A second step towards a safe implementation assessment is the definition of a typical railway infrastructure. The idea is to play the scenario on an infrastructure embedding the main design assumptions which are used in the considered railway line. The specification of this infrastructure has to be detailed such a way that the simulation can be considered as realistic.

Then, we are facing a security problem related to industrial confidentiality. It may be dangerous and consequently forbidden, to communicate safety critical information corresponding to an industrial infrastructure.

The proposed solution is to identify a virtual infrastructure which is fully documented in order to be able to communicate. This infrastructure was named an "academic benchmark", as it allows testing some technologies and scenarios avoiding all problems mentioned above [2].

The result of the study is the specification of a typical scenario that can be played on a typical infrastructure. Then, this system can be modelled using various modelling tools in order to assess various safety related aspect of the system [3]. Anyway, this academic benchmark is one of the main deliverable embedding most of the safety related industrial needs.

Proposing a safety methodology using several formal methods is the challenging goal of the next study.

Bibliography

[1] English section of: http://www.bea-tt.developpement-durable.gouv.fr/saint-romain-en-gier-r21.html

[2] Sun, Pengfei, Simon Collart-Dutilleul, and Philippe Bon (2014). "Formal modeling methodology of French railway interlocking system via HCPN". In: *COMPRAIL 14, International conference on Railway Engineering Design and Optimization*. Rome, Italy (cit. on pp. 4, 50, 65, 74, 102)

[3] Bon, Philippe, Simon Collart-Dutilleul, and Pengfei Sun (2013). "Study of implementation of ERTMS with respect to French national rules using a B centred methodology". In: *Industrial Engineering and Systems Management (IESM 2013)*, pp. 1–5 (cit. on p. 4)