2SC5891 – Design of a safe signaling system for the railways

Instructors: Idir Ait Sadoune
Department: DOMINANTE - INFORMATIQUE ET NUMÉRIQUE
Language of instruction: FRANCAIS
Campus: CAMPUS DE PARIS - SACLAY
Workload (HEE): 40
On-site hours (HPE): 27,00

Description

The aim is to discover critical systems modeling activities in railway systems, by using the CLEARSY Safety Platform and by proving some safety properties. During this project, several safety functions will be developed, implemented and improved, mainly using Boolean expressions. Such a system usually has hundreds or thousands of equations, it is understood that this project addresses only a subset of them.
Signaling system control is a risky activity since an error could allow:
- a train derailing.
- two trains colliding.
We will focus on the logical functions that allow a train to make a safe trip for the chosen route topology.

Quarter number

ST5

Prerequisites (in terms of CS courses)

- Design and verification of critical systems (the specific course of the ST)
- Modeling by using B method (to be done at the first day of this ST)

Syllabus

- - Modeling a critical system by using the B formal method, the Atelier B tool, and the Clearsy Safety platform.
- - Modeling a railway system.
- - Modeling and Verification of the safety properties of a railway system.
- - Generating a source code to be embedded in an electronic card from a B formal model.

Class components (lecture, labs, etc.)

Project over a week (9 half days)

Grading

- Students will be evaluated after a presentation of the obtained results (15 or 20 minutes).

Resources

- Atelier B, a tool enabling the operational use of B method. (https://www.clearsy.com/outils/atelier-b/)
- Clearsy Safety Platform (https://www.clearsy.com/outils/clearsy-safety-platform/).

Learning outcomes covered on the course

Learning outcomes targeted in the course:

- - Modeling a critical system using the B formal method.
- - Modeling Safety properties in the railway systems.
- - Verification of Safety properties by using theorem proving.
- - Generating a source code to be embedded in an electronic card from a B formal model.

Description of the skills acquired at the end of the course

- C1 - Analyze, design, and build complex systems with scientific, technological, human, and economic components
- C2 - Develop in-depth skills in an engineering field and a family of professions
- C4 - Have a sense of value creation for his company and his customers
- C6 - Be operational, responsible, and innovative in the digital world
- C7 - Know how to convince