ST5 – 58 – COMPLEX INDUSTRIAL AND CRITICAL SYSTEMS WITH DOMINANT SOFTWARE

Dominante : Info&Num (Computer and Digital)
Langue d'enseignement : Freench
Campus où le cours est proposé : Paris-Saclay

Engineering problem

This thematic sequence approaches an axis of software sciences through the implementation of a development cycle allowing the design of complex industrial and critical systems where software is preponderant. Modern industrial systems are often composed of heterogeneous interacting components that can be defined as complex systems (systems of systems). What characterizes such systems is that they are often software dominated (e.g. cyber-physical systems). Moreover, their behavior is often difficult to apprehend because of the emergence of global behaviors that cannot be anticipated at a more local level. Finally, they are critical in the sense that the slightest design error can have crippling consequences on the global behavior of the system.

More precisely, this thematic sequence aims at addressing both the design and the verification of such complex and critical systems by using techniques from Software Engineering. As the components of such systems are heterogeneous (i.e. both physical and software), the methodologies and tools presented in this topic will be multiple and will be integrated in a development cycle. The idea is to start the analysis phase using semi-formal tools (UML, SysML, ...), often used in systems engineering to describe the structuring of the system and its interactions, and then to scientifically approach the design and validation phases using formal techniques of Software Engineering (timed and hybrid modeling, temporal logic, model-checking) The interaction of the system with its external environment (which can be the human user or not) is one of the main points that will be taken into account.

The main objective of such an approach is to show, through the formal models obtained, that the system does what is expected of it while respecting the constraints imposed by the specifications and by the environment, or in the opposite case, to extract the states of the system that may call into question its proper functioning. In the latter case, the economic gain is very interesting and appreciable by the engineers who will benefit from correcting the problems detected by the verification of the model before moving on to the implementation stage (programming).

Adviced prerequisites

None

Context and issue modules: This part is structured around half-days of training aimed at presenting the sequence, the integration teaching and introducing the theme. Thus, conferences and round tables will be organized on the current state of model-driven engineering in the industrial world and the challenges for the future; or entitled "The application of Formal Methods to Railway Signalling Software".

Specific course (60 HEE) : *Design and verification of critical systems*

Brief description: a critical system is a system whose failure can have serious consequences, such as transportation systems (trains, planes, cars ...) or energy production systems (nuclear, wind ...). These systems are complex and in order to guarantee their proper functioning, it is necessary to take into account the continuous and event-driven aspects of their dynamics. A part of the course will therefore be dedicated to the design and modeling of critical and complex systems. In addition, their reliability is a major economic and societal issue. Another part of the course will then be dedicated to the methods and tools (formal or semi-formal) proposed to guarantee the safety properties during the design phase.

Challenge week n°1: *Design of a safe signalling system for railways*

- Associated partner: Systerel

- Location: Paris-Saclay campus

Brief description: In a railway system, it is essential that the points do not move when a train runs over them, otherwise there is a high risk of derailing. To this end, a signaling system has signals (a bit like traffic lights on the road) that allow to ask trains to stop before the switches. Things get more complicated if the train is too close to the signal to stop (same problem as an orange light for a car). The objective of this case study is to formally model such a system and to show that it is safe: the trains will not derail.

Challenge week n°2: *Design of intelligent systems for automated air traffic control*

- Associated partner: to be confirmed

- Location: Paris-Saclay campus

- Brief description: Critical information systems in the avionics field are subject to very important time and reliability constraints. Their development therefore requires engineering techniques that take these characteristics into account from the early phases of their life cycle. This AR focuses on the design of models of intelligent systems to control air traffic and the verification of certain safety properties on these models. These systems implement many strongly interacting components, which are parallel and asynchronous. All these subsystems are subject to verification and testing to ensure their own functionality. For example, it is critical to demonstrate the absence of deadlocks and the ability of each to operate correctly within their own time constraints. It is also important to schedule the actions of these subsystems and ensure a reliable control of the whole system. As an example, some important properties (formulated in STL) to check: 1) Air traffic should never be allowed in both directions simultaneously on the same route 2) The aircraft must respond to messages within a limited time 3) For two aircraft, there must be a separation with a minimum distance.

Challenge week 3: *Design and analysis of production systems for smart factories*

- Associated partner: to be confirmed

- Location: Paris-Saclay campus

- Brief description: Industry 4.0 or "smart factories" are concepts that define the fourth industrial revolution, which began at the beginning of the 21st century and continues to develop. This revolution is deeply linked to the evolution of information and communication technologies (ITC). When these technologies are integrated into production systems, new characteristics appear. Indeed, production systems are not only able to communicate with other systems and their environment, but they are also able to make decisions at the local level. These characteristics allow for more flexibility and agility in production strategies and entail a need for flexible, low-volume, high-mix manufacturing in a highly uncertain environment in which planning and control of production under disruption becomes a decisive decision-making issue. In this AR, students will tackle, through specific case studies, typical problems in the design of flexible production systems (i.e. task scheduling problem in production, production robustness analysis, etc). Through modeling tools (e.g. probabilistic model checking) that allow to take into account different uncertainty factors, students will learn basic principles for performance analysis and optimization of these systems that are the basis of smart factories.