Thesis title: Fine-grained data-flow security in real-time critical systems (FILTRATE)
(Please find the French version below)

Contact: Alain Plantec (alain.plantec@univ-brest.fr), Hai Nam Tran (hai-nam.tran@univ-brest.fr)
Host institution: Université de Bretagne Occidentale (https://www.univ-brest.fr/)
Laboratory: Lab-STICC (https://www.labsticc.fr/)

Keyword: Security, Modeling, Verification, Real-time embedded systems

Candidate profile: It is preferable for a candidate to have an education or a first-time experience in one of the three domains below:

+ Embedded systems
+ Real-time systems
+ Modeling (languages and modeling tools)

A strong background in software engineering or security is well-appreciated.

Thesis description

Context: The thesis focuses on security in the context of real-time critical systems (RTCS). These systems are qualified as *real-time* because the usefulness of correct outputs either degrades or becomes meaningless if they are produced after a certain deadline. They are qualified as *critical* if the failure of such a system has unacceptable consequences for society. These systems consist of different tasks which can be executed simultaneously or in sequence, and can be synchronized according to a controlled schedule. They are, for example, implemented in autonomous vehicles, unmanned aerial vehicles, and robots. Their verification is largely based on the validation of timing properties. The designer has precise information concerning these properties which can either be expressed by modeling or computed by scheduling analysis.

Problem statement: Verification methods used for RTCS are mostly based on the validation of timing properties or schedulability. These methods are qualified as *early verification* because they are used during the design phase. However, considering hardware malfunctions, software malfunctions, or malicious cyberattacks, the early validation of timing properties is insufficient to guarantee the proper functioning of a system during operation. Indeed, at any moment, the data flow can be corrupted due to unforeseen alterations.

For example, an application malfunction or an intrusion attack can lead to:

- delayed data accesses (see Figure 1a),
- changes in the order of data accesses (see Figure 1b),
- absences of data accesses (see Figure 1c).

Therefore, it is necessary to be able to measure the possible timing deviations of data accesses, to control their nature, and to detect the additions or the absences of certain accesses.

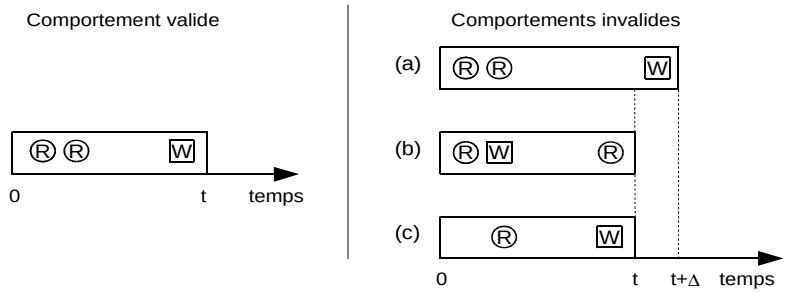

Figure 1: Example of invalid behavior detection w.r.t data accesses

General objectives: During operation, we can consider a RTCS as a graph of elements that interact by exchanging data. At any moment, its data can be altered. The cause of such an alteration can be a hardware or software malfunction or the result of a malicious attack. Recent studies have shown that there are different attack possibilities including hardware attacks, wireless network attacks, or sensor spoofing. The work carried out in this thesis aims to secure RTCS by applying a dynamic control on data accesses and scheduling. In other words, we verify at run-time whether data accesses are in accordance with the scheduling planned by the designer.

In this thesis, we need to find the answers for the following questions

a) How to quality the data of a given system by taking into account its timing properties.
b) How to control the validity of data accesses.
c) How to control the absence or the unexpected presence of data accesses?
d) How to instrument the implementation of real-time systems with techniques for controlling data accesses?
e) How to improve a real-time scheduling simulator to highlight possible deficiencies?

In RTCS, the execution of tasks is ensured by a scheduler which relies on the timing properties of the tasks it manages. Typically, a scheduler applies a scheduling policy that was validated during the system design phase. Thus, the scheduler has a global viewpoint on the whole system at run-time. The main idea of this thesis is to study how to exploit the scheduler and the knowledge of timing properties for a dynamic control of data accesses.

Expected contribution: The thesis will start with preliminary work to investigate and propose a method to model the relation between data accesses and timing properties of tasks in RTCS - the "time-data" relation. In other words, we aim to create an enriched task model for the analysis of RTCS by taking into account data accesses. Then, the model will be used to achieve two contributions.

Contribution 1: Design of components dedicated to monitoring and controlling data accesses. We aim to develop new data management patterns associated with the extensions of a modeling language (such as AADL - Architecture Analysis and Design Language), which allows the control and authorization of data accesses as a function of time. For example, prohibiting a task of modifying its data during a specific period or detecting the absence of certain data accesses.

Contribution 2: Security-aware scheduling simulation. It is necessary to have a simulation tool that allows us to verify the efficiency and correctness of the proposed monitoring components. The simulator should not only simulate data accesses but also dynamically introduce disturbances.

The PhD student will contribute to the development of the Cheddar project. This project, initiated in September 2000 at Lab-STICC, aims to increase the applicability of the real-time scheduling theory. In this project, we study how an architecture design language and real-time scheduling theory can help facilitate the verification of RTCS. Development activity is also carried out in a partnership with Ellidiss Technologies located in Brest.