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.

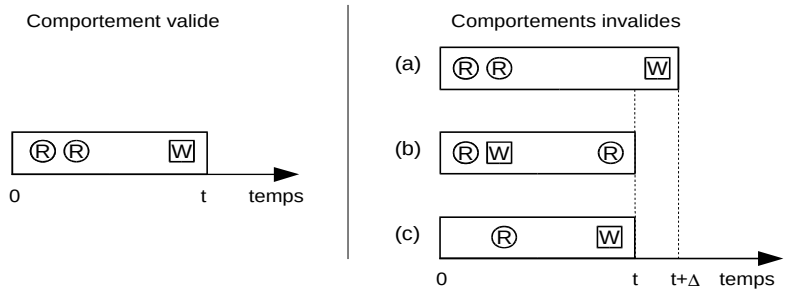

Figure 1: Example of invalid behavior detection w.r.t data accesses

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.

Titre de la thèse : Fine-grained data-flow security in real-time critical systems (FILTRATE)

Contact : Alain Plantec (alain.plantec@univ-brest.fr), Hai Nam Tran (hai-nam.tran@univ-brest.fr)
Établissement d'accueil : Université de Bretagne Occidentale (https://www.univ-brest.fr/)
Unité de recherche : Lab-STICC (https://www.labsticc.fr/)

Mots clés : Sécurité, Vérification, Modélisation, Systèmes temps réel embarqués

Profil et compétences recherchées :
- Le/la doctorant(e) devrait préférablement avoir une formation ou une première expérience dans l'un des domaines suivantes :
    + Système temps-réel
    + Architectures embarquées
    + Modélisation, c'est-à-dire connaissance des langages et outils de modélisation
- Les compétences en cybersécurité et génie logiciel sont appréciées

Descriptif de la thèse

Contexte : La thèse porte sur la cybersécurité dans les systèmes temps réel critiques. La validité de ces systèmes ne dépend pas seulement des valeurs des résultats produits, mais également des délais dans lesquels les résultats sont produits. Ils sont qualifiés de critiques car la défaillance d'un tel système a des conséquences inacceptables pour la société. De tels systèmes se composent de différentes tâches qui peuvent s'exécuter simultanément ou en séquence et peuvent être synchronisées suivant un ordonnancement contrôlé. Ils sont, par exemple, mis en œuvre pour les véhicules autonomes, les véhicules aériens sans pilote (UAV), ou les robots. Leur vérification repose actuellement en grande partie sur la validation des propriétés temporelles. Le concepteur dispose d'informations précises concernant ces propriétés qui peuvent être soit exprimées par modélisation, soit produites par analyse d'ordonnancement.

Problématique : Les méthodes les plus utilisées pour valider de tels systèmes visent notamment à garantir leurs propriétés temporelles. Ces méthodes de validation sont qualifiées de *précoces* car elles sont utilisées pendant la phase de conception des systèmes. Cependant, face à des dysfonctionnements matériels, des dysfonctionnements logiciels ou des attaques malveillantes, la validation précoce des propriétés temporelles est insuffisante pour garantir le bon fonctionnement d'un système en cours d'exploitation. En effet, à tout moment, un flux de données peut être corrompu à cause d'altérations imprévues.

Par exemple, un dysfonctionnement ou une attaque avec intrusion agissant par remplacement de certains composants peuvent conduire :
- à un retard des accès aux données (cf. Figure 1a),
- à des modifications de l'ordre des accès aux données (cf. Figure 1b),
- ou à des absences d'accès aux données (cf. Figure 1c).

Il faut donc être capable de mesurer le décalage temporel éventuel des accès aux données, de contrôler leur nature et de détecter l'ajout ou la suppression de certains accès aux données.

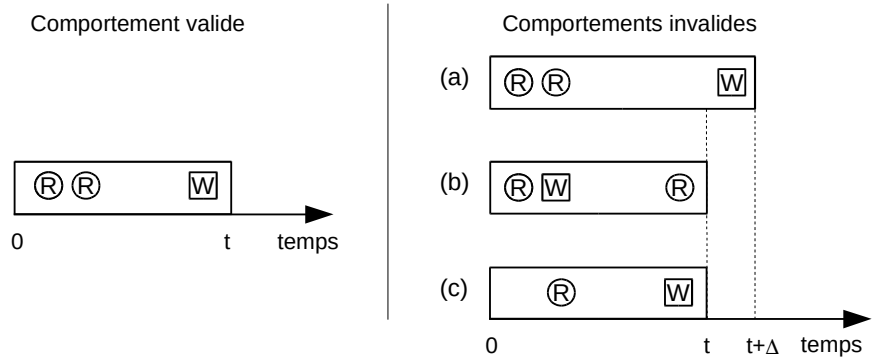

Figure 1 : Exemple de détections des comportements invalides en prenant en compte des opérations effectuées sur les données

Objectifs généraux : Les travaux menés pour cette thèse visent à accroître les capacités de vérification du fonctionnement d'un système par un contrôle dynamique des opérations effectuées sur les données et de leur ordonnancement : il s'agit donc de contrôler pendant l'exécution du système, que les opérations effectuées sur les données demeurent conformes à ce qui a été prévu par le concepteur.

En cours de fonctionnement, on peut considérer un système temps réel comme un graphe d'éléments qui interagissent par échange de données. À tout moment, une donnée peut être altérée. La cause d'une telle altération peut être un dysfonctionnement matériel ou logiciel ou encore la résultante d'une attaque malveillante. Des études récentes ont montré qu'il existe différentes possibilités d'attaque, notamment les attaques matérielles pures, les attaques par les réseaux sans fil et les attaques par altération des mécanismes de captation des données par les capteurs.

Pour ces travaux les questions soulevées sont les suivantes:

a) Comment qualifier les données en tenant compte du temps ?
b) Comment contrôler qu'une opération effectuée sur des données est valide à un moment donné ?
c) Comment contrôler l'absence ou la présence non anticipée de certains accès aux données ?
d) Comment instrumenter la mise en œuvre des systèmes temps réel avec des techniques de contrôle des opérations effectuées sur les données ?
e) Comment améliorer les simulateurs pour mettre en évidence les déficiences possibles ?

Dans un système temps réel, le contrôle de l'ordre d'exécution des tâches est assuré par un ordonnanceur qui s'appuie sur les propriétés temporelles des tâches qu'il gère. Classiquement, un ordonnanceur applique un modèle d'ordonnancement des tâches qui a été validé pendant la conception du système. L'ordonnanceur dispose donc d'un point de vue global sur l'ensemble du système en cours d'exécution : les tâches qui s'exécutent et leurs propriétés temporelles. L'idée directrice de cette thèse est d'étudier comment exploiter l'ordonnanceur et le modèle temporel qu'il est censé appliquer pour un contrôle dynamique des opérations effectuées sur les données.

Travail attendu : Les travaux s'appuieront sur des travaux préliminaires pour proposer une méthode de modélisation des relations entre les opérations effectuées sur les données, les tâches du système et les propriétés temporelles – les relations « temps-données ». En d'autres termes, nous visons à créer des modèles de tâches enrichis pour l'analyse de systèmes temps réel critiques en prenant en compte les opérations effectuées sur les données. Ces modèles seront ensuite utilisés pour atteindre les deux contributions suivantes.

Contribution 1 : *Conception de composants dédiés à la surveillance et au contrôle des accès aux données*. Développement de nouveaux patrons de gestion de données associées à des extensions

d’un langage de modélisation temps réel (comme AADL) permettant le contrôle et l'autorisation des injections, des lectures et des modifications en fonction du temps et des tâches pour par exemple interdire à une tâche de modifier une donnée pendant une période non autorisée ou détecter l’absence de certains accès aux données.

Contribution 2 : *Simulation d'ordonnancement.* Il est nécessaire de disposer d’un outil de simulation permettant de valider les composants dédiés à la surveillance des données et notamment, leurs propriétés temporelles. Cet outil devrait permettre non seulement de simuler les accès aux données, mais aussi d’introduire dynamiquement des perturbations pour mettre à l’épreuve le système.

La thèse se déroulera dans le cadre du projet Cheddar. Ce projet, initié en septembre 2000 au Lab-STICC, a pour objectif d'accroître l'applicabilité de la théorie de l'ordonnancement temps réel. Dans ce projet, nous étudions comment un langage de conception d'architecture peut contribuer à faciliter la vérification des performances d'un système temps réel critique avec la théorie de l'ordonnancement temps réel. Cette activité est conduite dans le cadre d'un partenariat avec la société *Ellidiss Technologies* située sur Brest. Les travaux menés durant cette thèse permettront d'élargir les contributions du projet Cheddar concernant la validation dynamique et la sécurisation des systèmes temps-réel critiques.