From static analyses to runtime verification of cyber-physical systems

Guillaume Roumage, Selma Azaiez, Stephane Louise

From Static Analyses to Runtime Verification of Cyber-Physical Systems

Guillaume Roumage[1], Selma Azaiez[1], Stéphane Louise[1]

[1] *University Paris-Saclay, CEA, List* F-91120, Palaiseau, France

{guillaume.roumage, selma.azaiez, stephane.louise}@cea.fr

Dataflow models belong to models that are used in a system to predict its behavior at design-time and to derive its static analyses. However, unaccounted runtime faults may undermine these static analyses. The static analysis performed remains valid at runtime if and only if some properties are valid at runtime. This poster presents a temporal logic to specify the monitoring of such properties.

Context and Motivations

Static analyses with dataflow models

Dataflow models provide a formalism to model Cyber-Physical Systems (CPS) with a directed graph. Dataflow models also help to ensure, at design-time, safety properties of CPS [1] such as:

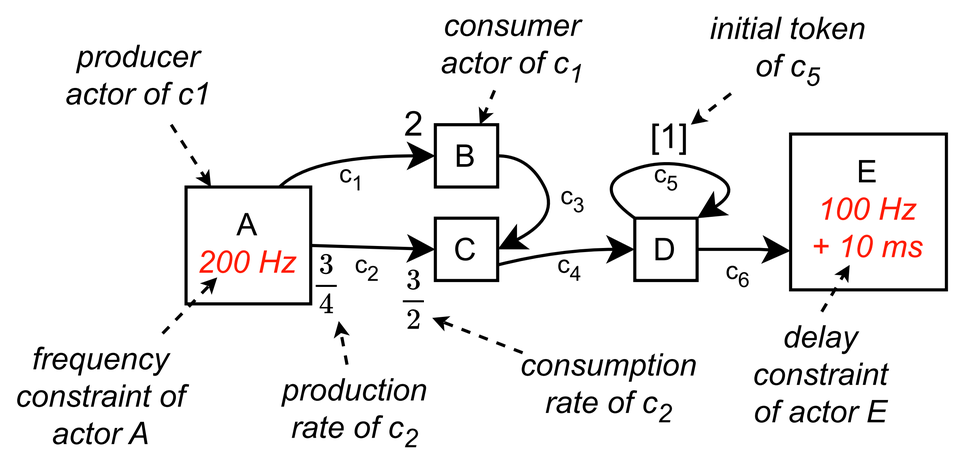
- Consistency: the system can run in finite memory.
- Liveness: the system does not have deadlocks.
- Data sequencing: compute the order in which the system's actors should process data at runtime.

Guaranteeing static analyses at runtime

- Our work assumes that the static analysis performed on a dataflow model is valid at runtime if and only some properties deduced from static analyses are also valid during runtime.
- We aim to detect unaccounted runtime faults that may undermine properties deduced from static analyses.

Consistency analysis with the PolyGraph model

Our work uses PolyGraph [2], a dataflow model tailored for Cyber-Physical Systems with timing constraints. Below is a simple PolyGraph model:



The consistency of the PolyGraph model is valid at runtime if within an execution:

1. the number of tokens produced and consumed matches the specifications;
2. the number of tokens in each channel regularly returns to an initial state.

Runtime Verification Framework

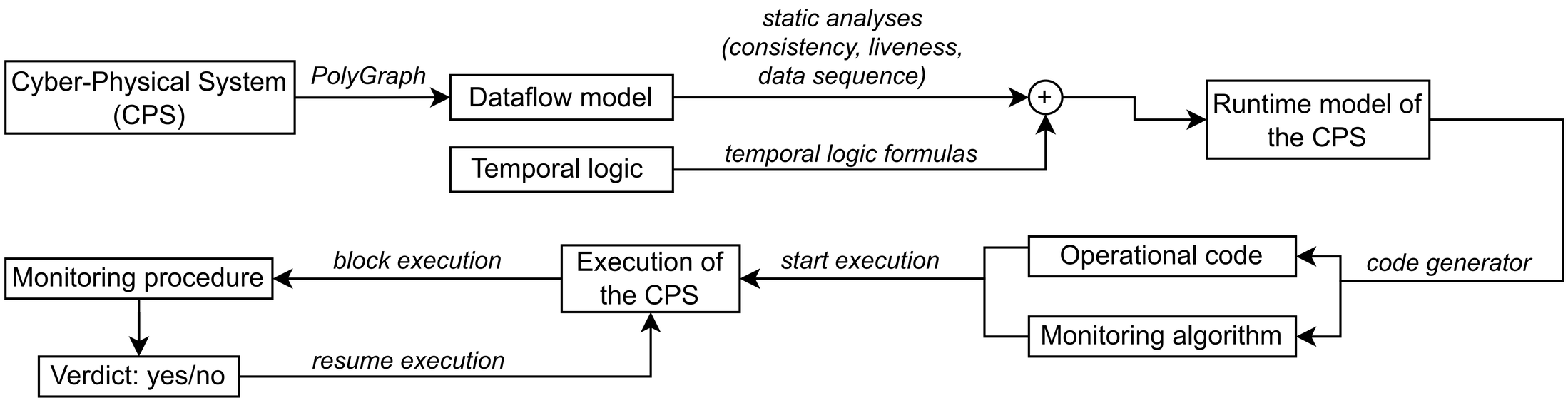
A temporal logic to specify the monitoring of dataflow models execution

We design a temporal logic to specify the monitoring of properties deduced from a consistency analysis. The syntax is: $\varphi = prod(c) \mid cons(c) \mid rv(a)$

- $prod(c)$ specifies the monitoring of the number of produced tokens in channel c;
- $cons(c)$ specifies the monitoring of the number of consumed tokens in channel c;
- $rv(a)$ specifies the monitoring of the number of tokens inside each input channel of actor a.

Given a consistent dataflow model, the monitoring of properties specified by $prod(c)$, $cons(c)$, and $rv(a)$ for all channels c and all actors a can detect runtime faults that may undermine the consistency of the dataflow model.

Overview of the runtime verification framework



Use case and Results

Use case: the Ingenuity Mars helicopter

- NASA has designed the Ingenuity Mars helicopter. Ingenuity computes its position, velocity, and altitude with an Inertial Measurement Unit and a Lidar. A Kalman filter fuses those measurements with vision processing results.
- We created an inspired dataflow model of Ingenuity from the textual specifications [3] [4]. We performed static analyses (consistency, liveness and data sequencing) of our model.

Results

We successfully monitor properties deduced from the consistency analysis of Ingenuity's dataflow model. It was evaluated in terms of:

- Accuracy: all injected faults are detected;
- Execution time: the difference between the execution time of a monitored and a non-monitored execution is negligible.
- Memory: the additional memory needed to monitor an execution is bounded.

[1] Lee, E., & Seshia, S. (2017). Introduction to Embedded Systems—A Cyber-Physical Systems Approach (Second Edition, Version 2.2). MIT Press.
[2] Dubrulle, P., Kosmatov, N., Gaston, C., & Lapitre, A. (2021). PolyGraph: A data flow model with frequency arithmetic. International Journal on Software Tools for Technology Transfer, 23(3), 489–517.
[3] Grip, H. *et al.* (2019). Flight Control System for NASA's Mars Helicopter. AIAA Scitech 2019 Forum.
[4] Grip, H. *et al.* (2019). Vision-Based Navigation for the NASA Mars Helicopter. AIAA Scitech 2019 Forum.