CPS: Medium: Resource-Aware Hierarchical Runtime Verification for Mixed-Abstraction-Level Systems of Systems

Kristin Yvonne Rozier[1] (PI), Phillip H. Jones[2] (Co-PI), Tichakorn Wongpiromsarn[3] (Co-PI), Iowa State University, Ames, IA
1) Department of Aerospace Engineering, 2) Department of Electrical & Computer Engineering, 3) Department of Computer Science

https://laboratory.temporallogic.org/publications/

Project overview

This project designs, analyzes, and implements fundamental runtime verification techniques by dealing with three general and orthogonal problems: mixed-abstraction-level granularity in specifications, resource-awareness to ensure non-intrusiveness of runtime monitors, and augmenting monitors with model-prediction to enable on-deadline mitigation triggering.

Challenges

Cyber-physical systems-of-systems require a specification language that allows reasoning over signals of different types (e.g., different time granularities or levels of abstraction), and for safety purposes, a manner of triggering mitigation strategies in a timely manner.

Scientific impacts

- **FO-logic constructs** in MLTL allow for less error prone authoring of CPS specifications
- **Explicit deadline** incorporation, and prediction in RV supports real-time system needs of CPS
- **MaxSAT** for MLTL could support future mechanisms for graceful degradation of CPS when all specifications cannot be met simultaneously

Solution

1) Improvements in formal specification entry to intuitively reason over sets, via C2PO interface, 2) Created an efficient and provably correct encoding of FO-logic constructs into MLTL, 3) Extended MLTL language to incorporate mitigation trigger deadlines, 4) Initial integration of deadlines into R2U2 RV engine, 5) Extended MaxSAT to MLTL

Intuitive Formal Specification with Efficient Encoding:

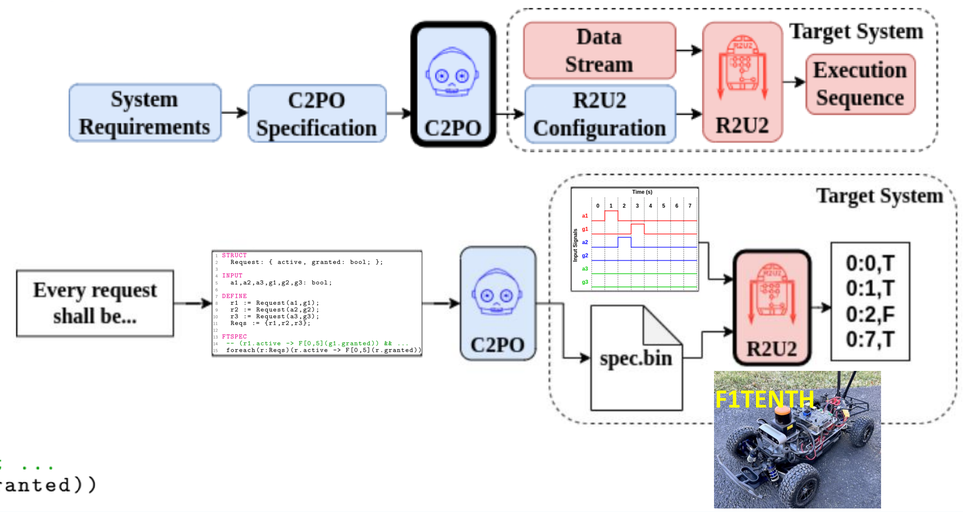
English Requirement

Every request shall be granted within 5s where only 3 requests can be queued at once.

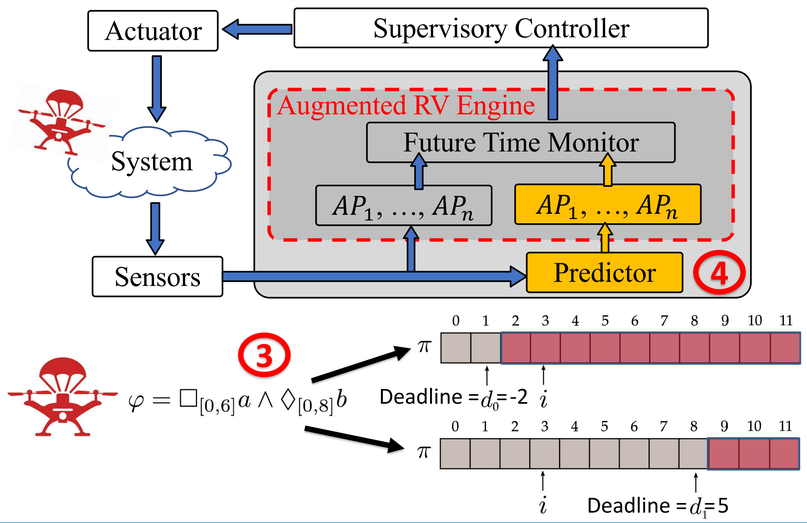
Enter as MLTL for C2PO compilation ①

```
1  STRUCT
2    Request: { active, granted: bool; };
3
4  INPUT
5    a1,a2,a3,g1,g2,g3: bool;
6
7  DEFINE
8    r1 := Request(a1,g1);
9    r2 := Request(a2,g2);
10   r3 := Request(a3,g3);
11   Reqs := {r1,r2,r3};
12
13 FTSPEC
14  --(r1.active -> F[0,5](g1.granted)) && ...
15  foreach(r:Reqs)(r.active -> F[0,5](r.granted))
```

② FO-LTL → Domain Constraints → MLTL



Model Predictive Runtime Verification (MPRV):



Broader impact on society

- Success of this project will reduce the complexity associated with specifying, implementing, and verifying CPS, thus aiding in the safe deployment of next generation CPS into society

Broader impact on education and outreach

- Four PhD students exposed to interdisciplinary research across Formal Methods, Controls, Embedded Systems (one female PhD student recruited)

Broader impact

- Support design & deployment of safer CPS into society
- Support robustness of CPS to off-nominal operating conditions

2024 NSF Cyber-Physical Systems Principal Investigators' Meeting
March 20 - 21, 2024

Award ID#: CNS-2038903