

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

Kristin Yvonne Rozier(PI), Phillip H. Jones(Co-PI), Tichakorn Wongpiromsarn(Co-PI), Iowa State University

Requirements

Challenge:

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)

Solution:

Introduced MLTL Multi-type (MLTLM), an extension of MLTL that

- includes type conversions between different types in one formula
- allows for changing type conversions
- cleanly separates type conversions from logic

E.g., DOORS, Project Lexical management "Verify that every day the plant is in production for at least one hourSystem Specification definition Sensor types, System MLTLSpec. differential equations engineer designer (Not a straightforward spec. in LTL/MLTL) Requirements Ex. DOORS, Project Lexical management "Verify that every day the plant is System Top view in production for at least one definition specification hourSensor types, System Formal MLTLM Spec. differential equations engineer spec. with rate designer $\sqcup_{[0,364,days]}\Diamond_{[0,23,hours]}$ plant-production Concrete specification Automation Encode "at least" and assistance 24 hrs = 1 day

Scientific Impact:

Syntax/semantics

- Formalize reasoning over signals of multiple types
- Simplify workflow for developing CPS specifications

Broader Impact:

- An open-source implementation of a direct encoding of MLTLM for runtime verification
- Involves 4 PhD students

Award ID#: CNS-2038903 Award Date: January 1, 2021