TU WIEN Informatics

SRDS 2022
41st International Symposium on Reliable Distributed Systems

Welcome to SRDS 2022
Vienna, Austria, September 19-22, 2022

doctoral college
RESILIENT EMBEDDED SYSTEMS

Fault Diagnostics for Safety-Critical Cyber-Physical Systems

Drishti Yadav

Technische Universität Wien
Institute of Computer Engineering
Cyber-Physical Systems Research Unit

Motivation

Verification and Validation (V&V) of Safety-critical Cyber-Physical Systems (CPS) is important.

Quick and correct detection and diagnosis of faults

Viable and fully operational at all times

Undetected failures: costly, life-threatening

Fail-safe design and Verification of safety aspects

- Model-based development
- MathWorks® MATLAB/Simulink
- System-under-test (SUT): Simulink models

Problem Statement

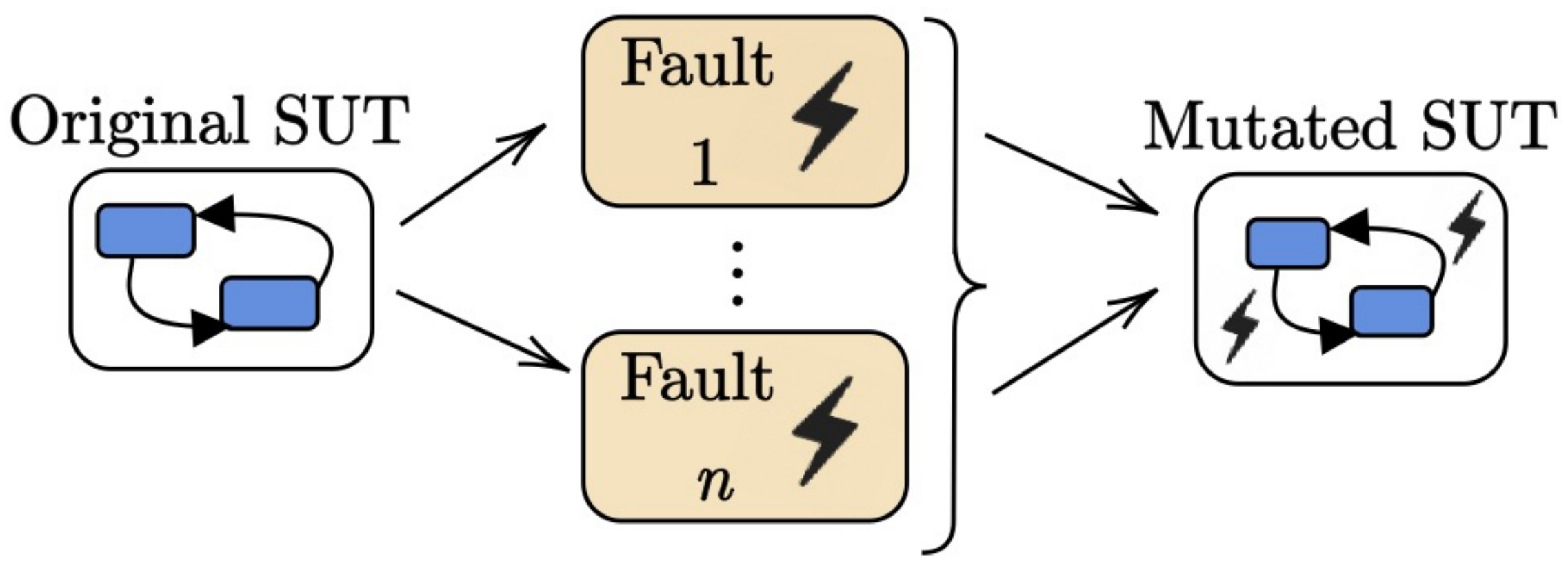
How does one determine the falsifying behavior and provide automated support for fault localization and failure explanation in CPS?

Research Questions

1. How to leverage automated and systematic **injection** of faults to allow scalable experiments?
2. How to improve CPS **falsification** and efficiently tackle the exploration-exploitation trade-off?
3. How to **localize** multiple faults accurately, improve the quality of failure explanation and provide an automated support for **debugging** faults?

Expected Results

- An automated and systematic toolkit to leverage fault injection in a SUT (i.e., a CPS designed in Simulink), allowing scalable experimentation and testing.



- Novel heuristic-driven algorithm(s) to aid falsification-based testing of CPS.
- Approach(es) to accurately localize multiple faults in a SUT at various hierarchical depths.
- Approach(es) to expose failures in CPS, refine failure explanation and provide automated debugging support.

State-of-the-art

Fault Injection and Mutation

- SIMULTATE [4], ErrorSim, FIBlock, MODIFI
- Not automated; Limited choice of fault types

CPS Falsification

- STL formalism [2]
- Metaheuristic algorithms
- Machine learning techniques

Fault Localization (FL)

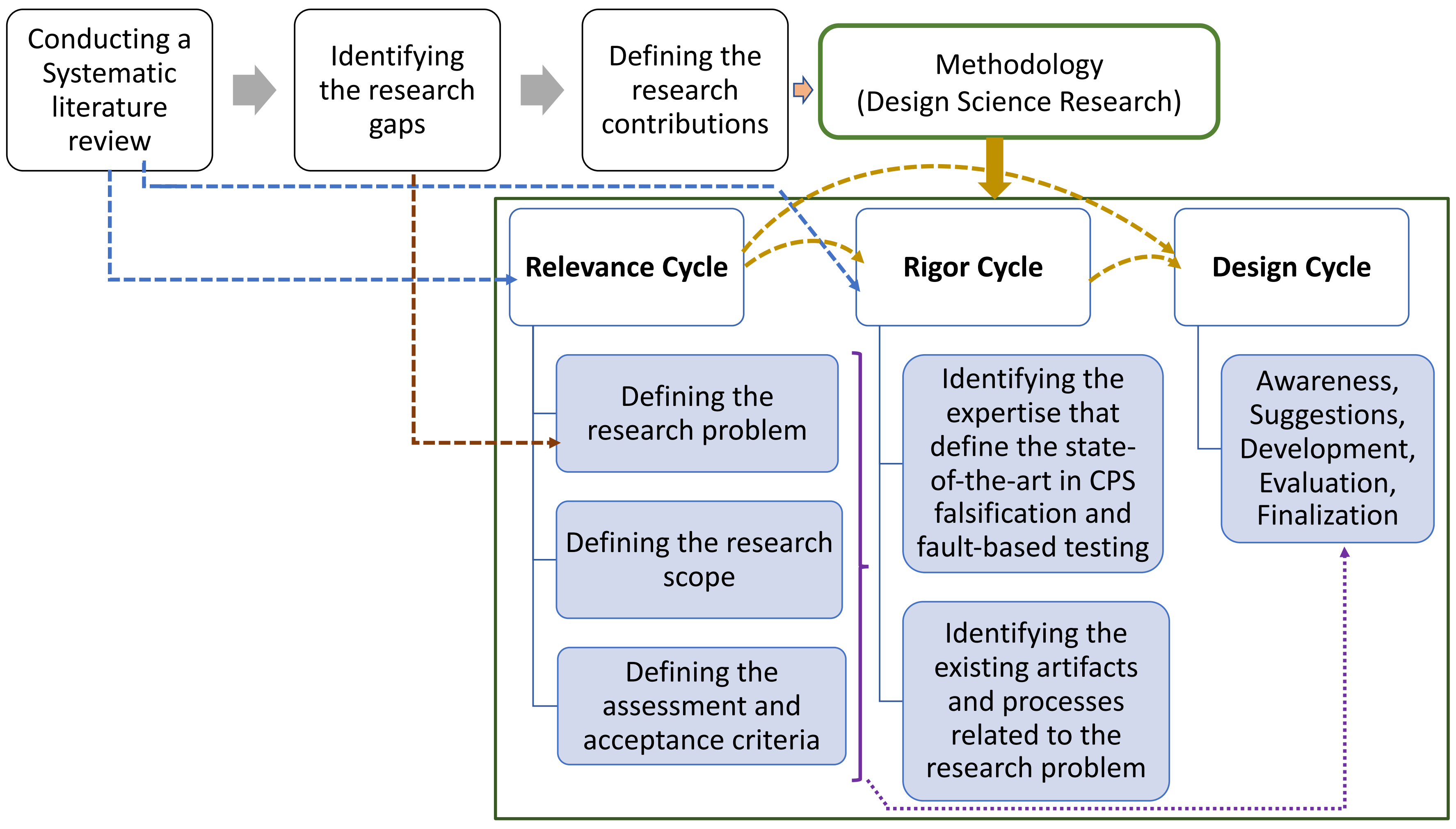
- Falsification, prediction models
- Statistical debugging
- Model slicing, CPSDebug [1]

Limitations of existing FL techniques

- Ad-hoc; Small number of fault models
- Single fault or multiple faults of the same type

Methodology

Based on **Design Science Research** methodology (by Hevner [3])


Conducting a Systematic literature review

Identifying the research gaps

Defining the research contributions

Methodology (Design Science Research)

Relevance Cycle

- Defining the research problem
- Defining the research scope
- Defining the assessment and acceptance criteria

Rigor Cycle

- Identifying the expertise that define the state-of-the-art in CPS falsification and fault-based testing
- Identifying the existing artifacts and processes related to the research problem

Design Cycle

- Awareness, Suggestions, Development, Evaluation, Finalization

Literature Survey

- Fault injection, CPS falsification, Fault localization
- V&V, Testing, Mutation analysis
- STL and diagnostics

Assessment

- Empirical evaluation using scalable experiments
- Open-source benchmarks
- Case-study based analysis

Approaches

- Search-based testing with STL
- Mutation testing
- Metamorphic testing

References

[1] Ezio Bartocci et al. "CPSDebug: Automatic failure explanation in CPS models". In: *International Journal on Software Tools for Technology Transfer* (2021).

[2] Alexandre Donzé and Oded Maler. "Robust satisfaction of temporal logic over real-valued signals". In: *FORMATS*. Springer. (2010).

[3] Alan R Hevner. "A three cycle view of design science research". In: *Scandinavian journal of information systems* (2007).

[4] Ingo Pill et al. "SIMULTATE: A Toolset for Fault Injection and Mutation Testing of Simulink Models". In: *ICSTW*. IEEE. (2016).

Publications

1. Drishti Yadav, "Blood Coagulation Algorithm: A novel bio-inspired meta-heuristic algorithm for global optimization," Mathematics, 9(23), 2021.
2. Ezio Bartocci, Leonardo Mariani, Dejan Nickovic, and Drishti Yadav, "FIM : Fault Injection and Mutation for Simulink", ESEC/FSE 2022.
3. Ezio Bartocci, Leonardo Mariani, Dejan Nickovic, and Drishti Yadav, "Search-based Testing for Accurate Fault Localization in CPS", ISSRE 2022.

Contact: drishti.yadav@tuwien.ac.at