Center for Embedded Systems
An NSF Industry/University Cooperative Research Center

# On the Verification of Formal Methods for Digital Embedded Control Systems

Dr. Dimitri Kagaris
Dr. Spyros Tragoudas
SIUC

SIU Southern Illinois University CARBONDALE

NATIONAL SCIENCE FOUNDATION

ASU Ira A. Fulton Schools of Engineering
ARIZONA STATE UNIVERSITY

# Project Overview and Description

## Modelling and checking of specifications and requirements

(i) specifications and requirements are constantly being changed/refined at least in the initial design phases;

(ii) conflicts/incompatibilities in the design can be found at an earlier stage;

(iii) reliability, performance and quality assurance standards are maintained throughout the design development

# Problem

**Amount of requirements can be huge.**

**How to cope with the capabilities of existing solvers/checkers.**

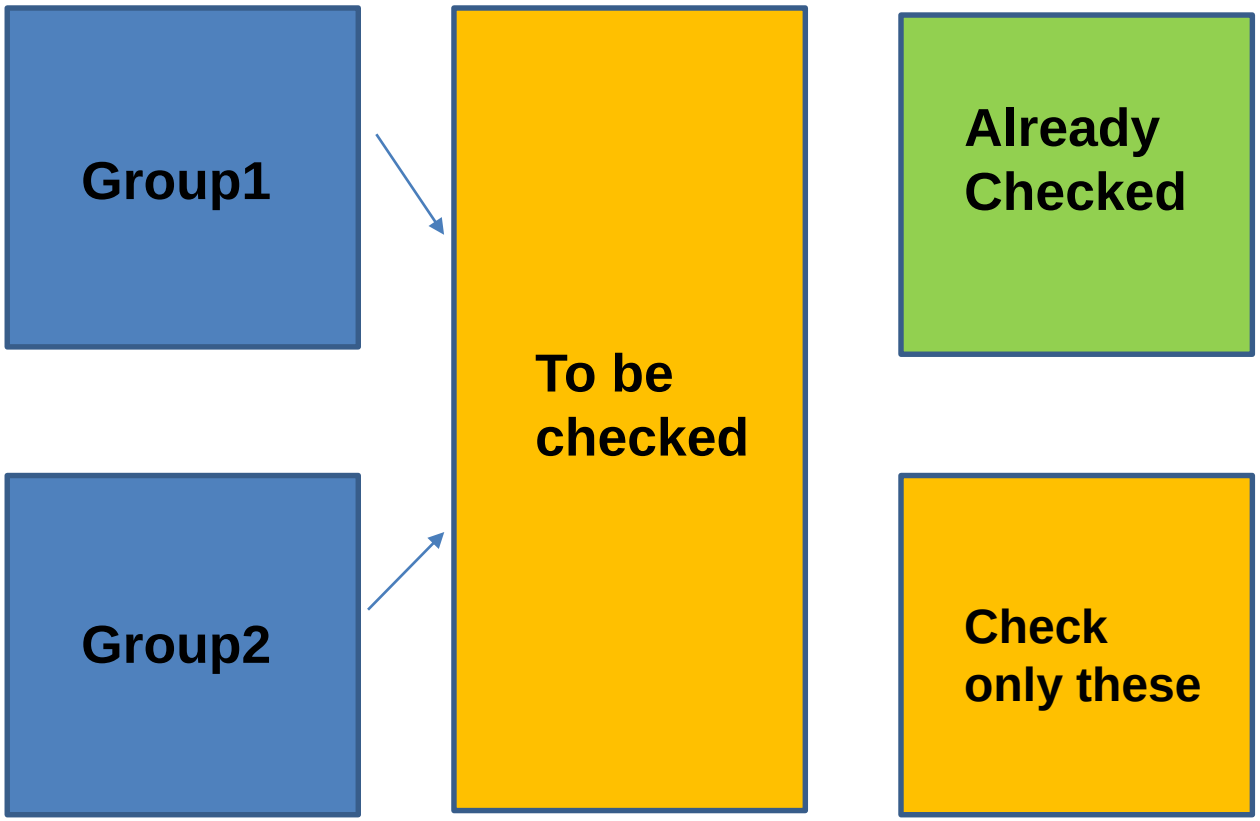
- ABsolver
- Prover9 / Mace4
- MathSAT
- Alt-Ergo
- SNARK
- PVS
- TPS
- Vampire
- E
- veriT
- Z3

# Approach

- Start from formal specification of requirements of a digital embedded control system (such as VDM, Z, SPARK)
- Investigate Existing Theorem Provers/Solvers/Checkers
- Develop procedures to make consistency check more scalable.
- Check the scalability on industrial case studies (avionics, automotive applications).

# Approach

## Incremental Verification/Consistency Check



# Novelty

- **Novelty**

  **Formal design verification/consistency check is not well studied in terms of scalability.**

  **This project will provide methodologies and results on specific industrial cases.**

# Project Tasks/ Deliverables

| | Description | Date | Status |
|---|---|---|---|
| 1 | Exploration of the capabilities of existing theorem provers/ solvers that can work in conjunction with Formal Methods. | Q1 | Not yet started |
| 2 | (Same as 1) | Q2 | Not yet started |
| 3 | Development of scalable procedures. | Q3 | Not yet started |
| 4 | Extensive experimentation for scalability analysis. | Q4 | Not yet started |

**Deliverables:**

- **Methodology for automatic verification/validation/consistency check of a large amount of formal requirements.**
- **Application of the approach on industrial case studies.**