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

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.

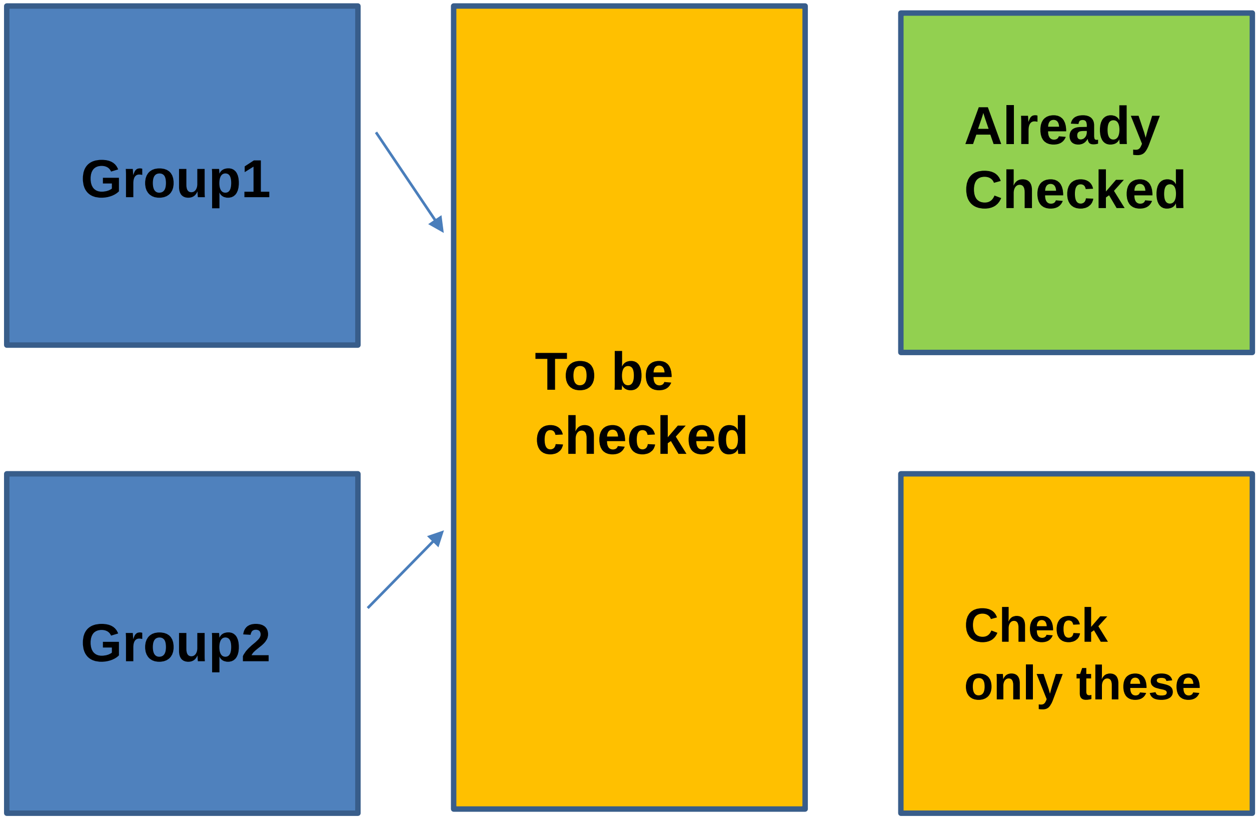
How to cope with the capabilities of existing solvers/checkers.

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



Group1

Group2

To be checked

Already Checked

Check only these

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.**

Theorem Provers/SMT solvers

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

Example

- Reaction1(A,B: SensorVal)

  post ((A >100) & (B <= 10))

- Reaction2(A,B,C: SensorVal)

  post (((A >100) | (B>2) | (C>10)) & ~ Reaction1(A,B))

- Reaction3(A,B: SensorVal)

  post ((A >150) & (B>4) & (B<=8))

- Reaction4(A,B,C: SensorVal)

  post ((C>10) &(~(A>100) | ~(B>2)))

- **Reaction3 incompatible with 1 and 2**
- **Reaction4 compatible with 1 and 2**

References

- 1. Maharaj, S.; Bicarregui, J., "On the verification of VDM specification and refinement with PVS," Proc. 12th IEEE International Conference on Automated Software Engineering, 1997, pp.280-289.
- 2. S. Agerholm and J. Frost. An Isabelle-based Theorem Prover for VDM-SL. In Proceedings
- of the 10th International Conference on Theorem Proving in Higher Order Logics (TPHOLs’97),
- Springer-Verlag LNCS, 1997
- 3. Fitzgerald, J.S., Larsen, P.G., Mukherjee, P., Plat, N. and Verhoef,M., Validated Designs for Object-oriented Systems. Springer Verlag 2005.
- 4. Bicarregui, J.C., Fitzgerald, J.S., Lindsay, P.A., Moore, R. and Ritchie, B., Proof in VDM: a Practitioner's Guide. Springer Verlag Formal Approaches to Computing and Information Technology (FACIT), 1994.
- 5. Breuer, P.T.; Madrid, N.M.; Sanchez, L.; Marin, A.; Kloos, C.D., "A formal method for specification and refinement of real-time systems," Proceedings of the Eighth Euromicro Workshop on Real-Time Systems, pp.200-204, 12-14 Jun 1996.
- 6. Nieuwenhuis, R.; Oliveras, A.; Tinelli, C. (2006), "Solving SAT and SAT Modulo Theories: From an Abstract Davis-Putnam-Logemann-Loveland Procedure to DPLL(T)", Journal of the ACM 53 (6), pp. 937–977.
- 7. Susmit Jha, Rhishikesh Limaye, and Sanjit A. Seshia. Beaver: Engineering an efficient SMT solver for bit-vector arithmetic. In Proceedings of 21st International Conference on Computer-Aided Verification, pp. 668–674, 2009.
- 8. Larsen, P.G.; Lausdahl, K.; Battle, N., "Combinatorial Testing for VDM,"), 2010 8th IEEE International Conference on Software Engineering and Formal Methods (SEFM, 278-285, 13-18 Sept. 2010
- 9. Aoyama, M.; Tanabe, H., "A Design Methodology for Real-Time Distributed Software Architecture Based on the Behavioral Properties and Its Application to Advanced Automotive Software," 2011 18th Asia Pacific Software Engineering Conference (APSEC), pp.211-218, 5-8 Dec. 2011
- 10. Guo Xie; Xinhong Hei; Mochizuki, H.; Takahashi, S.; Nakamura, H., "Formalizing and Analyzing the Train-to-Wayside Network System for CBTC," 2012 Workshop on Dependable Transportation Systems/Recent Advances in Software Dependability, pp.15,22, 18-19 Nov. 2012.
- 11. Nielsen, C.B.; Larsen, P.G., "Extending VDM-RT to enable the formal modelling of System of Systems," 2012 7th International Conference on System of Systems Engineering (SoSE), pp.457-462, 16-19 July 2012.
- 12. Isasa, Jose Antonio Esparza; Jorgensen, Peter Wurtz Vinther; Larsen, Peter Gorm, "Hardware In the Loop for VDM-real time modeling of embedded systems," 2014 2nd International Conference on Model-Driven Engineering and Software Development, pp.209-216, 7-9 Jan. 2014.