Center for Embedded Systems (CES)
Request for Proposals Template – YEAR 7

DUE: Monday, April 1, 2015, by 5 p.m.

TITLE:	**On the Verification of Formal Methods for Digital Embedded Control Systems**				
PI:	Dimitri Kagaris Spyros Tragoudas	**EMAIL:**	kagaris@engr.siu.edu spyros@engr.siu.edu	**TEL:**	618-453-7973 618-453-4027
DEPT:	Electrical and Computer Engineering	**SCHOOL:**	Southern Illinois University Carbondale		

ABSTRACT: (250 OR FEWER WORDS)

Specifications and requirements for embedded control systems need typically to be modelled at a higher level than that of the implementation for several reasons: (i) specifications and requirements are constantly changed/refined at least in the initial design phases; (ii) conflicts/incompatibilities in the design can be found at an earlier stage; (iii) descriptive and notational formalisms are needed so that reliability, performance and quality assurance standards are maintained throughout the design development. Several formal methods have been developed for this purpose, including the VDM and Z formal languages. Although these languages provide formal semantics that allow in principle the proof and verification of the properties of the model, they are not accompanied by adequate tools to support automatic verification. In this project, we propose to investigate existing approaches and develop new ones in order to aid the automatic verification/validation/consistency check of the requirements, as they are dynamically developed in the design modelling process of digital embedded control systems.

PROBLEM:

Formal design specification methods like the VDM and Z formal languages allow in principle the proof and verification of the properties of the design model, but existing tools for automatic proof (like the PVS and Isabelle-based theorem provers) are not adequate and/or are not addressing the specific needs of specific digital embedded control systems.

RATIONALE:

Identifying the specific needs of an embedded control system and customizing an automatic proof method that can be used in each particular case is a promising way to provide the much needed verification/validation/consistency check

APPROACH:

Given a formal specification of requirements of a digital embedded control system in a formal language such as VDM, we will investigate how well the requirements can be modeled and verified/validated using the powerful Satisfiability Module Theories (SMT) and Boolean Satisfiability (SAT) methods. Trade-offs in applicability and computation complexity will also be investigated.

Consider the following example from a hypothetical chemical plant:
Reaction 1 is to take place when Sensor A > 100 and Sensor B <10.
Reaction 2 is to take place when Sensor A > 100 or Sensor B > 2 or Sensor C > 10 but in no case when Reaction1 is taking place.
These requirements can be modelled in VDM as implicit functions (with post-conditions) as follows:

```
Reaction1(A,B: SensorVal)
post ( (A >100) & (B <= 10) )
```

Reaction2(A,B,C: SensorVal)
post (((A >100) | (B>2) | (C>10)) & ~ Reaction1(A,B))

Now assume that an additional requirement is imposed that a third reaction Reaction3 must take place simultaneously with Reaction2, whenever Sensor A > 150 and Sensor B is between 4 and 8, i.e.,

Reaction3(A,B: SensorVal)
post ((A >150) & (B>4) & (B<=8))

By translating these post-condition requirements in logic we find that the newly added Reaction3 cannot occur simultaneously with Reaction2 (A must be A>150 and B must be B <= 8, but Reaction2 requires that Reaction1 is not activated, i.e., A<=100 or B > 10).

However, if instead of Reaction3 we had a Reaction4 with the requirement that it should occur simultaneously with Reaction 2 whenever Sensor C > 10 and at least one of Sensors A and B is below the corresponding threshold needed for Reaction2, i.e.,

Reaction4(A,B,C: SensorVal)
post ((C>10) &(~(A>100) | ~(B>2))),

then the logic checking can show that this is consistent when C > 10 and A <= 100 (indeed by expanding the expression for the negation of Reaction1 in Reaction2 and the negation of A>100 in Reaction4, it can be seen that the expression (A<=100) & (C>10) appears in the expression for Reaction2 as well as in the expression for Reaction4.

NOVELTY:

Existing tools for automatic proof (like the PVS and Isabelle-based theorem provers) are not adequate and/or are not addressing the specific needs of specific digital embedded control systems for formal verification. This project will provide methodologies and results on specific industrial cases.

POTENTIAL BENEFITS TO INDUSTRY MEMBERS:

Formal design specification is much in demand and the present study will provide additional insight in the automatic verification process.

DELIVERABLES:

The deliverables for this project are as follows:

1. A methodology for automatic verification/validation/consistency check of formal requirements.
2. Application of the approach on an industrial case studies.

TIMELINE/MILESTONES: (PER QUARTER)

The timeline for the first four quarters of this project is as follows:

1. Quarters 1,2: Exploration of the capabilities of existing theorem provers/SAT solvers that can work in conjunction with Formal Methods.
2. Quarters 3,4: Development and application of SMT/SAT based method and application to industrial cases.

TECHNOLOGY TRANSFER:

Technology transfer will be performed in the form of comprehensive reports.

BUDGET:

Funds in the amount of $25,000 are requested for:

1. Support of two graduate students, PI salaries.
2. Travel to Industrial Advisory Board (IAB) meetings and member company locations for in-person meetings as required

BIBLIOGRAPHY: (ATTACH IN IEEE CONFERENCE OR JOURNAL FORMAT)

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.

.

I/UCRC Executive Summary - Project Synopsis		**Date: 04/01/15**
Project Title: On the Verification of Formal Methods for Digital Embedded Control Systems		
Center/Site: Center for Embedded Systems/Southern Illinois University Carbondale		
Principle Investigator: Dimitri Kagaris Spyros Tragoudas		**Type: Continuing**
Tracking No.: (CES office to input)	**Phone :** 618-453-7973 618-453-7027	**E-mail :** kagaris@engr.siu.edu spyros@engr.siu.edu
		Proposed Budget: $25,000

Abstract: Specifications and requirements for embedded control systems need typically to be modelled at a higher level than that of the implementation for several reasons: (i) specifications and requirements are constantly changed/refined at least in the initial design phases; (ii) conflicts/incompatibilities in the design can be found at an earlier stage; (iii) descriptive and notational formalisms are needed so that reliability, performance and quality assurance standards are maintained throughout the design development. Several formal methods have been developed for this purpose, including the VDM and Z formal languages. Although these languages provide formal semantics that allow in principle the proof and verification of the properties of the model, they are not accompanied by adequate tools to support automatic verification. In this project, we propose to investigate existing approaches and develop new ones in order to aid the automatic verification/validation/consistency check of the requirements, as they are dynamically developed in the design modelling process of digital embedded control systems.

Problem: Formal design specification methods like the VDM and Z formal languages allow in principle the proof and verification of the properties of the design model, but existing tools for automatic proof (like the PVS and Isabelle-based theorem provers) are not adequate and/or are not addressing the specific needs of specific digital embedded control systems.

Rationale / Approach: Identifying the specific needs of an embedded control system and customizing an automatic proof method that can be used in each particular case is a promising way to provide the much needed verification/validation/consistency check. Given a formal specification of requirements of a digital embedded control system in a formal language such as VDM, we will investigate how well the requirements can be modeled and verified/validated using the powerful Satisfiability Module Theories (SMT) and Boolean Satisfiability (SAT) methods. Trade-offs in applicability and computation complexity will also be investigated.

Novelty: Existing tools for automatic proof (like the PVS and Isabelle-based theorem provers) are not adequate and/or are not addressing the specific needs of specific digital embedded control systems for formal verification. This project will provide methodologies and results on specific industrial cases.

Potential Member Company Benefits: Formal design specification is much in demand and the present study will provide additional insight in the automatic verification process.

Deliverables for the proposed year: The deliverables for this project are (1) a methodology for automatic verification/validation/consistency check of formal requirements and (2) application of the approach on an industrial case studies.

Milestones for the proposed year: Quarters 1 and 2: Exploration of the capabilities of existing theorem provers/SAT solvers that can work in conjunction with Formal Methods. Quarters 3 and 4: Development and application of SMT/SAT based method and application to industrial cases.

Progress to Date: THIS SECTION TO BE UPDATED IN JANUARY

Estimated Start Date: 08/15/2015

Estimated Knowledge Transfer Date: 08/31/2016

PI INFORMATION: (ATTACH 2-PAGE CV)

Short Curriculum Vitae

DIMITRI KAGARIS
Professor
Department of Electrical & Computer Engineering
Southern Illinois University
Carbondale, IL 62901, USA
tel: (618)453-7973
fax: (618)453-7972
e-m: kagaris@engr.siu.edu

Dimitri Kagaris received the Diploma degree in Computer Engineering and Informatics from the University of Patras, Greece, in 1988, and the M.S. and Ph.D. degrees in Computer Science from Dartmouth College, Hanover, New Hampshire, USA, in 1991 and 1994, respectively.
He is currently a full professor in the Electrical & Computer Engineering Department, Southern Illinois University, Carbondale, Illinois, USA. His research interests include multicore systems, digital design automation and test, VLSI synthesis, computer networks.
He has over 80 publications in peer-reviewed journals and conferences and has contributed chapters in scientific encyclopedias. He has been active in the area of Built-in Self-Test and Design for Testability since 1992. Part of his research has been supported by National Science Foundation (NSF). He has received twice the Outstanding Paper Award from the IEEE International Conference on Computer Design. He has served as a reviewer in major journals and conferences and has participated three times in NSF panels for the review and funding of Design Automation proposals. He is currently serving as Associate Editor of the IEEE Transactions on Computers.

RECENT RELEVANT JOURNAL PUBLICATIONS

1. D. Kagaris, ``Maximizing the Lifetime of a Wireless Sensor Network with Fixed Targets," **Ad Hoc and Sensor Wireless Networks**, v. 17, n. 3-4, pp. 253 - 268, 2013.

2. D. Nikolos, D. Kagaris, S. Sudireddy, S. Gidaros, ``An Improved Search Method for Accumulator-Based Test Set Embedding," **IEEE Transactions on Computers**, v. 58, n. 1, pp. 132 - 138, Jan. 2009.

3. J. Kakade, D. Kagaris, D.K. Pradhan, ``Evaluation of Generalized LFSRs as Test Pattern Generators in Two-Dimensional Scan Designs," **IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems**, v. 27, n. 9, pp. 1689 - 1692, Sept. 2008.

4. J. Kakade, D. Kagaris, “Minimization of Linear Dependencies through the Use of Phase Shifters,” **IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems,** v. 26, n. 10, pp. 1877-1882, Oct. 2007.

5. D. Kagaris, T. Haniotakis, ``A Methodology for Transistor-Efficient Supergate Design,'' **IEEE Transactions on VLSI Systems**,v. 15, n. 4, pp. 488-492, Apr. 2007.

6. D. Kagaris, ``Improved TDM Switching Assignments for Variable and Fixed Burst Length,'' **International Journal of Satellite Communications and Networking**, v. 25, pp. 93-107, 2007.

7. D. Kagaris, P. Karpodinis, D. Nikolos, ``A Method for Accumulator-Based Test-per-Scan BIST,'' **IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems**, v. 25, n. 11, pp. 2578-2586, Nov. 2006.

8. D. Kagaris, S. Tragoudas, S. Kuriakose, “InTeRail: A Test Architecture for Core-Based SOCs,” **IEEE Transactions on Computers**, v. 55, n. 2, pp. 137-149, Feb. 2006.

9. D. Kagaris, “Phase Shifter Merging,” **Journal of Electronic Testing: Theory and Applications**, vol. 21, n. 2, pp. 161-168, April 2005.

10. D. Kagaris, “A Unified Method for Phase Shifter Computation**,” ACM Transactions on Design Automation of Electronic Systems**, vol. 10, no. 1, pp. 157-167, Jan. 2005.

11. D. Kagaris, “Multiple-Seed TPG Structures,” **IEEE Transactions on Computers**, vol. 52, no. 12, pp. 1633-1639, Dec. 2003.

12. D. Kagaris, S. Tragoudas “On the Non-Enumerative Path Delay Fault Simulation Problem,” **IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems**, vol. 21, n. 9, pp. 1095-1100, Sep. 2002.

13. D. Kagaris, “Linear Dependencies in Extended LFSMs,” **IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems**, vol. 21, n. 7, pp. 852-858, July 2002.

SPYROS TRAGOUDAS

PROFESSIONAL AFFILIATION AND CONTACT INFORMATION

Electrical & Computer Engineering Department, Southern Illinois University, Carbondale, IL 62901, ENGR-E, Rm 113, MC 6603, tel: (618) 453 7027, e{mail: spyros@engr.siu.edu, fax (618) 453 7972

EDUCATION

1986 Diploma (5 years), Computer Engineering and Informatics Department, University of Patras, Greece

1988 M.S., Erik Jonsson School of Engineering and Computer Science, Computer Science Program, The University of Texas at Dallas, Richardson, TX 75083-0688.

1991 Ph.D., Erik Johnson School of Engineering and Computer Science, Computer Science Program, The University of Texas at Dallas, Richardson, TX 75083-0688.

PROFESSIONAL EXPERIENCE

07/01/12 – current Professor and Chair, Electrical & Computer Eng. Dept., Southern Illinois University Carbondale

03/01/09-current Director, NSF IUCRC on Embedded Systems, SIUC-site.

07/16/99- current Professor, Electrical & Computer Eng. Dept., Southern Illinois University Carbondale.

08/16/98-07/15/99 Associate Professor, Electrical and Computer Engineering Department, University of Arizona.

08/16/91-08/15/98 Associate Professor, Computer Science Department, Southern Illinois University Carbondale (Assistant Professor until 6/30/96).

07/01/97-08/15/98 Graduate Program Director, Computer Science Department, Southern Illinois University Carbondale.

01/03/87-08/14/91 Research/Teaching Assistant, Computer Science Program, School of Engineering and Computer Science, The University of Texas at Dallas, Richardson, TX 75083-0688.

08/15/86-01/02/87 Systems Analyst, Computer Technology Institute, Patras, Greece.

RESEARCH INTERESTS

Design and Test Automation for VLSI, Embedded Systems

RESEARCH SPONSORS

Direct support: National Science Foundation, US Navy, SAIC, Intel, Qualcomm, Synopsys

NSF IUCRC: NSF, NAVSEA Crane, Rockwell Collins, United Technologies Aerospace Systems, SAIC, Intel, Caterpillar, TSI, EMAC, Wildlife Materials

PROFESSIONAL SERVICE

Editorial Board: IEEE Transactions on Computers, VLSI Design journal, Journal of electrical and Computer Engineering, Universal Computer Science, Research Letters in Electronics.

General Chair of IEEE DFTS 2010, Program Committee Chair of DFTS 2009, Program Committee member of many International Conferences

Has graduated 14 PhD students and supervised over 60 MS theses. Currently advising 11 PhD students

PUBLICATIONS

Over 70 journal papers and over 130 articles in peer-reviewed conference proceedings

Ten recent journal publications

• A.K. Palaniswamy and S.Tragoudas, An Efficient Heuristic to Identify Threshold Logic Functions, ACM Journal on Emerging Technologies in Computing (JETC), to appear in 2012.

• M.N. Skoufis, S. Tragoudas, An on-line Failure Detection Method for Data Buses using Multi-threshold Receiving Logic, IEEE Transactions on Computers, vol. 61, no. 2, pp. 187-198, Feb. 2012

• K. Stewart, Th. Haniotakis, and S. Tragoudas, Securing sensor networks: A novel approach that combines encoding, uncorrelation, and node disjoint transmission, Ad Hoc Networks, vol. 10, issue 3, May 2012, pp. 328-328, Elsevier.

• M.N. Skoufis, K. Karmakar, S. Tragoudas, and T. Haniotakis, A data capturing method for buses on chip, IEEE Transactions on Circuits and Systems I, vol. 57, no. 7, pp.1631-1641, July 2010.

• D. Jayaraman, R. Sethuram, and S. Tragoudas, Scan Shift Power Reduction by Gating Internal Nodes. J. Low Power Electronics 6(2): 311-319 (2010).

• E. Flanigan, S, Tragoudas, Path Delay Measurement Techniques using Linear Dependency Relationships, IEEE Transactions on VLSI Systems, vol. 18, issue 6, pp.1011-1015, June 2010.

• R. Adapa, S. Tragoudas, Techniques to Prioritize Paths for Diagnosis, IEEE Transactions on VLSI Systems, vol. 18, issue 4, pp. 658-661, April 2010.

• K. Christou, M. K. Michael, and S. Tragoudas, On the Use of ZBDDs for Implicit and Compact Critical Path Delay Fault Test Generation, Journal of Electronic Testing: Theory and Applications, 2008.

• A. Abdulrahman and S. Tragoudas, Low-Power Multi-Core ATPG to Target Concurrency, Integration, the VLSI Design Journal, vol. 41, issue 4, pp. 459-473, July 2008.

• C. Song, S. Tragoudas, Identification of Critical Executable Paths at the Architectural Level, IEEE Transactions on Computer Aided Design of Integrated Circuits and Systems (TCAD), vol. 27, no. 12, pp. 2291-2302, December 2008