Center for Embedded Systems (CES)
Request for Proposals Template – YEAR 8

DUE: FRIDAY, APRIL 15, 2016, by 11 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 difficult to use in practice as they require extreme formalism. In this project, we propose (i) to develop a supporting tool that can translate requirements specified in a more natural language to the formal input required by a theorem prover; (ii) to investigate the capabilities a specific publicly available theorem prover (Z3 of Microsoft Research) to verify/check for consistency the given requirements; (iii) to develop a new Binary Decision diagram (BDD) based approach to handle incrementally new requirements as they are dynamically developed in the design modeling process of digital embedded control systems, and (iv) compare the performance of the incremental approach to the static approach.

PROBLEM:

Formal design specification methods like the VDM formal language allow in principle the proof and verification of the properties of the design model, but existing tools for automatic proof do not provide a "natural" way for engineers to specify their requirements in practice and/or are not addressing the specific needs of digital embedded control systems, like the incremental addition/revision of requirements.

RATIONALE:

In an ideal world, requirements should not have to be so strictly described but they should always be strictly checked. To help bridge this gap, we propose to develop a tool that can translate from a "semi-formal" description of requirements to the extremely formal description that a theorem prover/solver needs. In addition, the requirements are constantly changed/revised during project development. Therefore, the benefits of an incremental approach over the standard approach of checking all requirements again from scratch is worth investigating.

APPROACH:

Part1: Translation from Natural Language.

Consider the following semi-formal way of describing requirements for an example power system monitor:

R1: [Average Main Frequency] shall be an average of the last 3 readings of [In XMS Frequency].

R2: [Main Power OverFrequency Condition] shall be set TRUE when [Average Main Frequency] is greater than 125Hz else it is set to FALSE.

R3: [Main Power OverFrequency Fault] shall be set TRUE when [Main Power OverFrequency Condition] is set to TRUE for 1 Second else it is set to FALSE.

R4: [Monitor Fault] shall be set TRUE when any of the following exist else it is set to FALSE:
[UnderFequency Fault] is set to TRUE.
[OverFequency Fault] is set to TRUE.
[OverCurrent Fault] is set to TRUE.
[UnderVoltage Fault] is set to TRUE.
[OverVoltage Fault] is set to TRUE.

R5: [Out XRM Close] shall be set TRUE when all of the following exist:
[Good Power] is set to TRUE.
[In XPOS] is set to FALSE.
[Monitor Fault] is set to FALSE.

We propose to take such a rather "natural" description (i.,e., not extremely formal as, for example, in the case of the VDM language) and transform it into something more formal like the following:

R1: = _AverageMainFrequency_ = (_InXMSFrequency_(t)_ + _InXMSFrequency_(t-1)_ + _InXMSFrequency_(t-2)_) / 3

R2: = _MainPowerOverFrequencyCondition_ = (_AverageMainFrequency_ > 125 Hz)

R3: = _MainPowerOverFrequencyFault_ = (_MainPowerOverFrequencyCondition_ AND (_DURATION_MainPowerOverFrequencyCondition_ = 1 Sec))

R4: = _MonitorFault_ = _UnderFequencyFault_ OR _OverFequencyFault_ OR _OverCurrentFault_ OR _UnderVoltageFault_ OR _OverVoltageFault_

R5: = _OutXRMClose_ = _GoodPower_ AND ~_InXPOS_~ AND ~_MonitorFault_

Such a format as the above which is more mathematically formal can then be used to further translate into the format required by a specific solver (such as Z3).

A tool for the translation from a natural language-like description such as the above has to tackle several points, such as:

(1) Extract variables,; (2) Check for variable naming inconsistencies (3) Handle the type and values of variables (logical or arithmetic); (4) Recognize "any" and "all" requirements; (5) Handle the occurrence of composite operations like "average"; (6) Handle timing durations (such as "TRUE for 1 Sec").

Part 2: Incermental Checker

For the incremental checker we propose the following (consult Fig. 1):

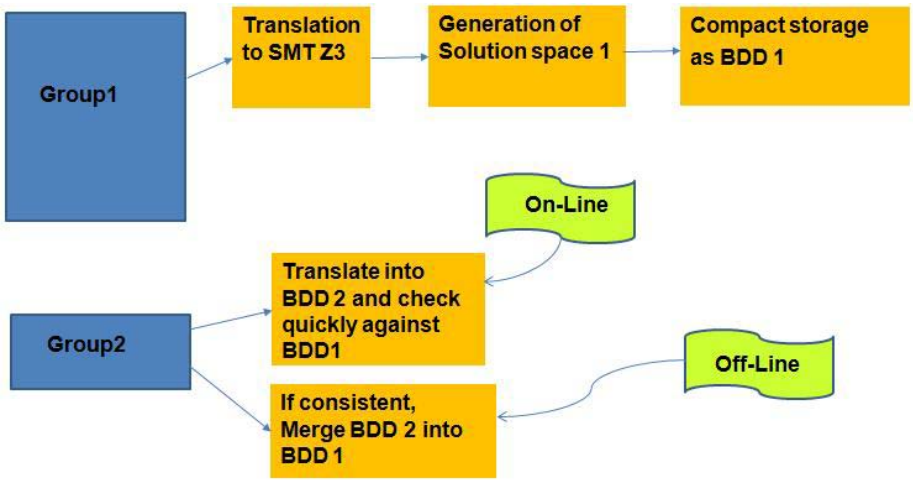

Fig.1: Incremental Approach

Assume that a set Group1 of requirements has already been checked by a solver like the SMT (Satisfiability Modulo Theories) solver Z3. If a new set Group2 of requirements comes, then we want to investigate if it is preferable to check via Z3 all the requirements in Group1 and Group2 as a whole, or to check the requirements in Group2 only, store the current solutions of Group2 (and Group1) via Binary Decision Diagrams (BDDs) and then check the resulting BDDs for consistency.

NOVELTY:

We propose a tool that can translate from a "semi-formal" description of requirements to the complete formal description that a theorem prover/solver (specifically Z3) needs. We also investigate the incremental approach in requirements checking.

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 tool for translation of requirements form natural-language to formal specification.
2. Application of Z3 and investigation of its capabilities on industrial case studies.
3. Investigation of the incremental approach in requirements checking.

TIMELINE/MILESTONES: (PER QUARTER)

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

Quarters 1 and 2: Translation tool.

Quarters 3 and 4: Implementation and investigation of the incremental approach.

TECHNOLOGY TRANSFER:

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

BUDGET:

Funds in the amount of $35,000 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. Nikolaj Bjørner and Anh-Dung Phan and Lars Fleckenstein. nu-Z: An Optimizing SMT Solver. TACAS April 2015.

2. Leonardo de Moura and Nikolaj Bjørner. Satisfiability modulo theories: introduction and applications. Commun. ACM, 54(9):69-77, 2011.

3. 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.

4. 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

5. Fitzgerald, J.S., Larsen, P.G., Mukherjee, P., Plat, N. and Verhoef,M., Validated Designs for Object-oriented Systems. Springer Verlag 2005.

6. 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.

7. 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.

8. 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.

9. 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.

10. 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

11. 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

12. 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.

13. 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.

14. 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: 04/13/16
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 modeled 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 difficult to use in practice as they require extreme formalism. In this project, we propose (i) to develop a supporting tool that can translate requirements specified in a more natural language to the formal input required by a theorem prover; (ii) to investigate the capabilities a specific publicly available theorem prover (Z3 of Microsoft Research) to verify/check for consistency the given requirements; (iii) to develop a new Binary Decision diagram (BDD) based approach to handle incrementally new requirements as they are dynamically developed in the design modeling process of digital embedded control systems, and (iv) compare the performance of the incremental approach to the static approach.

Problem: Formal design specification methods like the VDM formal language allow in principle the proof and verification of the properties of the design model, but existing tools for automatic proof do not provide a "natural" way for engineers to specify their requirements in practice and/or are not addressing the specific needs of digital embedded control systems, like the incremental addition/revision of requirements.

Rationale / Approach: we propose to develop a tool that can translate from a "semi-formal" description of requirements to the extremely formal description that a theorem prover/solver needs. In addition, the requirements are constantly changed/revised during project development. Therefore, the benefits of an incremental approach over the standard approach of checking all requirements again from scratch is worth investigating.

Novelty: We propose a tool that can translate from a "semi-formal" description of requirements to the extremely formal description that a theorem prover/solver (specifically Z3) needs. We also investigate the incremental approach in requirements checking.

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 ar: (1) tool for translation of requirements form natural-language to formal specification. (2) Application of Z3 and investigation of its capabilities on an industrial case studies. (3) Investigation of the incremental approach in requirements checking

Milestones for the proposed year: Quarters 1 and 2: Translation tool. Quarters 3 and 4: Implementation and investigation of the incremental approach.

Progress to Date: **THIS SECTION TO BE UPDATED IN JANUARY**

Estimated Start Date: 08/15/2016	**Estimated Knowledge Transfer Date**: 08/31/2017

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. O. Acevedo, D. Kagaris, ``On The Computation of LFSR Characteristic Polynomials for Built-In Deterministic Test Pattern Generation,'' **IEEE Transactions on Computers**, v. 65, n. 2, pp. 664-669, Feb. 2016.

2. D. Kagaris, ``MOTO-X: A Multiple-Output Transistor-Level Synthesis CAD Tool,'' **IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems**, v. 35, n. 1, pp. 114-127, Jan. 2016.

3. M. J. Rene, D. Kagaris, ``Equitable Shortest Job First: A Preemptive Scheduling Algorithm for Soft Real-Time Systems,'' **International Journal of Engineering Research and Innovation**, v.6, n.1, pp. 15--22, 2014.

4. 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.

5. 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.

6. 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.

7. 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.

8. 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.

9. 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.

10. 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.

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

12. 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.

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

14. 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.

15. 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