AFRL-AFOSR-VA-TR-2019-0092

Cyber-Physical Systems Specification Mismatch and Safe Upgrades

Christoph Csallner
UNIVERSITY OF TEXAS AT ARLINGTON
1 UNIVERSITY OF TEXAS AT ARL
ARLINGTON, TX 76019-0001

04/14/2019
Final Report

Air Force Research Laboratory
AF Office Of Scientific Research (AFOSR)/RTA2

Arlington, Virginia 22203
Air Force Materiel Command

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
14-04-2019	Final Performance	15 Aug 2015 to 14 Aug 2018

4. TITLE AND SUBTITLE
Cyber-Physical Systems Specification Mismatch and Safe Upgrades

5a. CONTRACT NUMBER

5b. GRANT NUMBER
FA9550-15-1-0258

5c. PROGRAM ELEMENT NUMBER
61102F

6. AUTHOR(S)
Christoph Csallner, Taylor Johnson

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
UNIVERSITY OF TEXAS AT ARLINGTON
1 UNIVERSITY OF TEXAS AT ARL
ARLINGTON, TX 76019-0001 US

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
AF Office of Scientific Research
875 N. Randolph St. Room 3112
Arlington, VA 22203

10. SPONSOR/MONITOR'S ACRONYM(S)
AFRL/AFOSR RTA2

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
AFRL-AFOSR-VA-TR-2019-0092

12. DISTRIBUTION/AVAILABILITY STATEMENT
A DISTRIBUTION UNLIMITED: PB Public Release

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Air Force cyber-physical systems (CPS) such as manned and unmanned aerial systems (UAS) and satellite constellations are composed of legacy and novel systems over at times decades-long lifespans. In this research, novel methods are developed to ensure such CPS have assurance to meet their design and mission requirements and only these in spite of potential design defects and bugs, attacks, and failures. The outcomes of the project include theoretical and practical tools to safely integrate legacy and new systems.

15. SUBJECT TERMS
Cyber-Physical System, Scalable Formal Methods

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			NGUYEN, TRISTAN
Unclassified	Unclassified	Unclassified	UU		19b. TELEPHONE NUMBER *(Include area code)* 703-696-7796

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18

Cyber-Physical Systems Specification Mismatch and Safe Upgrades

Final Report for Period: August 15, 2015 to August 14, 2018

Principal Investigator: Dr. Taylor T. Johnson (via subcontract)
Institution: Vanderbilt University, Electrical Engineering and Computer Science
Principal Investigator: Dr. Christoph Csallner
Institution: University of Texas at Arlington, Computer Science and Engineering
Award Number: FA9550-15-1-0258
Program Manager: Tristan Nguyen (previously James Lawton and Kathleen Kaplan), Systems and Software
Award Period: August 15, 2015 to August 14, 2018

1. Research Overview

Air Force cyber-physical systems (CPS) such as manned and unmanned aerial systems (UAS) and satellite constellations are composed of legacy and novel systems over at times decades-long lifespans. In this research, novel methods are developed to ensure such CPS have assurance to meet their design and mission requirements and only these in spite of potential design defects and bugs, attacks, and failures. Developing theoretical and practical tools to safely integrate legacy and new systems will help enable the Air Force goal to fly, fight, and win … in air, space, and cyberspace. This research investigated scalable formal methods and software engineering techniques to enable safe CPS upgrades through four major objectives, by: (1) defining cyber-physical specifications mismatches, and next ensuring no mismatches exist through (2) specification and invariant inference and (3) randomized differential testing, all to be conducted in conjunction with (4) a rigorous evaluation on CPS with prototypical features of Air Force CPS.

In more detail, the primary objectives undertaken are as follows.

- **Objective 1:** Defined cyber-physical specification mismatches, which are scenarios where assumptions on the systems' physical environments have been implicitly encoded in software and no longer hold due to cyber or physical upgrades, and are frequent sources of software-induced disasters (such as Ariane 5 flight 501) and hazards (such as recent NHTSA automotive recalls).
- **Objective 2:** Developed a specification inference framework to find cyber-physical specifications from models and CPS implementations, building upon tools such as invariant inference, dynamic analysis, and static analysis, implemented in a publicly available software tool called Hynger (for hybrid invariant generator).
- **Objective 3:** Developed a randomized differential testing framework for CPS development environments to identify specification mismatches in CPS and bugs in CPS development tools using a novel way to compare simulators using reachability analysis of hybrid automata, implemented in a publicly available software tool called Hyrg (for hybrid random generator).
- **Objective 4:** Evaluated the cyber-physical specification mismatch framework, specification inference framework, and randomized differential testing framework on challenging CPS case studies with Air Force relevance, particularly distributed swarm robotics systems using quadrotor drones.

During the project, each of the four major objectives was undertaken. For Objective 1, case studies and benchmarks were developed for defining cyber-physical specification mismatches, and

a formalization of the cyber-physical specification mismatch problem has been defined using an extension of hybrid input/output automata (HIOA) [26]. For Objective 2, a software tool called Hynger was developed and evaluated for its effectiveness in automating detection of cyber-physical specification mismatches and in its use in detecting other anomalous runtime scenarios, particularly possible attacks on sensors [21, 26]. A software tool called HyST was extended and evaluated to enable translation between different development tools for cyber-physical systems, particularly integrating with Simulink/Stateflow from the MathWorks, which is commonly used in development of CPS [6, 4]. For Objective 4, case studies and benchmarks using indoor quadcopters and DC electric microgrids have been conducted to evaluate the framework for defining and automatically detecting cyber-physical specification mismatches. These efforts resulted in several accomplishments as detailed below, including journal publications [20, 4, 41, 26, 38, 36, 40], conference publications [7, 5, 30, 32, 14, 35], workshop publications [31, 34, 8, 27], and releases of the software tools. The HyST software tool was recognized with a Best Software Repeatability award at 19th ACM International Conference on Hybrid Systems: Computation and Control (HSCC 2016) [5]. Rigorous definitions of cyber-physical specifications and mismatches have been investigated, using expressive formal languages such as signal temporal logic (STL) as well as invariants. The approach is implemented for cyber-physical mismatch detection in the Hynger tool, an overview of which appears in Figure 1.

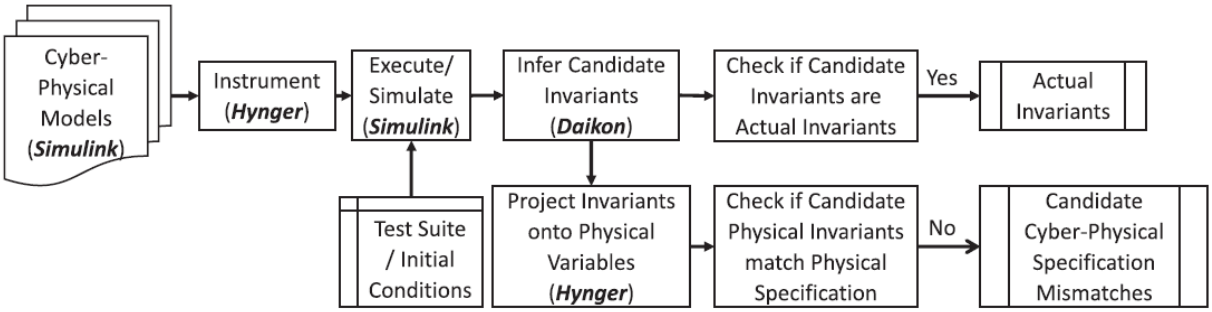

Figure 1: Overview of Hynger approach for automatically inferring specifications from CPS models and implementations, then checking if cyber-physical specification mismatches exist.

2. Motivation and Examples

Physical systems are becoming increasingly dependent upon computers and software, such as in emerging embedded and cyber-physical systems (CPS), where networked software interacts with physical processes. For instance, typical modern airplanes and cars utilize dozens-to-hundreds of microprocessors, many communications buses, and a complex interconnection between sensors, actuators, and processors [12, 11, 13]. In the design and development process for most engineered systems today (including CPS), the vast majority of resources are devoted to ensuring systems meet their specifications [10, 33]. In spite of significant technical advances for design verification and validation—such as model checking, hardware-in-the-loop testing, automatic test case generation for software, and sophisticated simulators—there are frequent safety recalls across CPS industries due to problems between cyber and physical subcomponents. For example, the Consumer Product Safety Commission (CPSC) has recalled between 2010-2012 fire alarm and control systems from Bosch, Tyco-Grinnell, and Honeywell for failure to sound alarms and/or notify fire departments [15, 16, 17], the Food and Drug Administration (FDA) has reported the leading cause of recent medical device recalls are cyber-related (tied with manufacturing defects) [3, 2], and the National Highway Traffic Safety Administration (NHTSA) has recalled hundreds of thousands of 2004-2005 and 2010-2014 Toyota Priuses due to drivetrain software problems

causing unexpected stalls [24, 28] and millions of 2005-2010 Hondas due to electronic control model software causing transmission damage [25]. Given that such recalls are due to increased risk of physical safety (and not yet, e.g., for privacy issues), all such problems are inherently cyber-physical.

2.1. Cyber-Physical Design Reuse and Upgrades

A recent example of a design-reuse problem is the NHTSA recall of 1.5 million Honda vehicles (including one of the author's) due to electronic control module (ECM) software problems that could damage the car's transmission, resulting in possible stalls [25]. The root cause of the safety defect was the result of a physical component (a bearing in the transmission) being upgraded to an improved design between different model-year vehicles without appropriate ECM software updates. Specifically: "Beginning with model year 2005 4-cylinder Accord and Element vehicles, specifications for the secondary shaft bearing outer race material and shape were modified in order to accommodate increased engine torque. These modifications, which improved the long-term durability of the component but reduced its resistance to shock, are not appropriately addressed in the automatic transmission control module software of the affected vehicles." [25] This problem was widespread in part because there was a five year delay before the problem was identified, and it was used across model makes and years (e.g., from $2005-2010$ model year Accords, $2007-2010$ CR-Vs, and $2005-2008$ Elements). This difficulty in root-cause analysis emphasizes the point such problems are probably underreported, and the reuse of components in CPS can lead to widespread serious problems.

Similar design-reuse problems have famously occurred in aviation—the Ariane 5 flight 501 disaster was a result of reusing Ariane 4's software without appropriate updates for the increased thrust of the new rocket [23, 1, 18, 22]. The following quotations from the inquiry into the cause of Ariane 5 flight 501's failure [1] highlight the issues with cyber-physical reuse and specification mismatches (emphasis added):

- "The design of the **Ariane 5** SRI [Inertial Reference System] is practically the same as that of an SRI which is presently used on **Ariane 4**, *particularly as regards the software*."
- "The value of BH [Horizontal Bias] was much higher than expected because the early part of *the trajectory of **Ariane 5** differs from that of **Ariane 4*** and results in *considerably higher horizontal velocity values*."
- "**Ariane 5** has a *high initial acceleration* and a trajectory which leads to a *build-up of horizontal velocity which is five times more rapid* than for **Ariane 4**. The *higher horizontal velocity* of **Ariane 5** generated, within the 40-second timeframe, leads to the excessive value which caused the inertial system computers to cease operation."
- "In **Ariane 4** flights using the same type of inertial reference system there has been no such failure because the trajectory during the first 40 seconds of flight is such that *the particular variable related to horizontal velocity cannot reach*, with an adequate operational margin, a value beyond the limit present in the software."
- "The reason for the three remaining variables, including the one denoting horizontal bias, being unprotected was that further reasoning indicated that they *were either physically limited or that there was a large margin of safety*, a reasoning which in the case of the variable BH turned out to be faulty."

Here, software made assumptions about the physical dynamics of the rocket, but the software was reused from Ariane 4, while Ariane 5 had greater thrust, so this assumption was invalid. Left unaddressed, issues related unstated assumptions in components are likely to get worse in such future CPS, where changes can occur in the software and hardware.

In this project, by addressing the four major research objectives outlined earlier, we made both theoretical and practical advances in defining and addressing this problem to ensure CPS may be safely upgraded with either physical and/or cyber component changes. The results of the project are summarized in the accomplishments listed next below, and the primary publication outcome of this project is a detailed journal article on cyber-physical specification mismatches [26].

3. Accomplishments and Personnel

The following list summarizes papers, other accomplishments, software artifacts, and personnel supported in part by this research effort during this project.

3.A. Publications – Journal Articles

- Luan Viet Nguyen, Khaza Hoque, Stanley Bak, Steven Drager, Taylor T. Johnson, "Cyber-Physical Specification Mismatches", In ACM Transactions on Cyber-Physical Systems (TCPS), 2018. [26] http://www.taylortjohnson.com/research/nguyen2018tcps.pdf
- Weiming Xiang, Hoang-Dung Tran, Taylor T. Johnson, "Output Reachable Set Estimation and Verification for Multi-Layer Neural Networks", In IEEE Transactions on Neural Networks and Learning Systems (TNNLS), 2018. [41] http://taylortjohnson.com/research/xiang2018tnnls.pdf
- Weiming Xiang, Diego Manzanas Lopez, Patrick Musau, Taylor T. Johnson, "Reachable Set Estimation and Verification for Neural Network Models of Nonlinear Dynamic Systems", In Unmanned System Technologies: Safe, Autonomous and Intelligent Vehicles, Springer, 2018, September. http://www.taylortjohnson.com/research/xiang2018ust.pdf
- Weiming Xiang, Hoang-Dung Tran, Taylor T. Johnson, "Nonconservative Lifted Convex Conditions for Stability of Discrete-Time Switched Systems under Minimum Dwell-Time Constraint", In IEEE Transactions on Automatic Control (TAC), 2018, September. [36] http://www.taylortjohnson.com/research/xiang2018tac_b.pdf
- Weiming Xiang, Hoang-Dung Tran, Taylor T. Johnson, "Robust Exponential Stability and Disturbance Attenuation for Discrete-Time Switched Systems under Arbitrary Switching", In IEEE Transactions on Automatic Control (TAC), 2018, May. [38] http://www.taylortjohnson.com/research/xiang2018tac_a.pdf
- Omar Ali Beg, Luan Viet Nguyen, Taylor T. Johnson, Ali Davoudi, "Signal Temporal Logic-based Attack Detection in DC Microgrids", In IEEE Transactions on Smart Grids (TSG), Institute of Electrical and Electronics Engineers (IEEE), 2018, April. [9] http://www.taylortjohnson.com/research/beg2018tsg.pdf
- J. A. Rosenfeld, R. Kamalapurkar and W. E. Dixon, "The State Following Approximation Method," in IEEE Transactions on Neural Networks and Learning Systems. doi: 10.1109/TNNLS.2018.2870040 http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8509137&isnumber=6104215
- Taylor T. Johnson, Stanley Bak, Marco Caccamo, Lui Sha, "Real-Time Reachability for Verified Simplex Design", In ACM Transactions on Embedded Computing Systems

(TECS), ACM, vol. 15, no. 2, New York, NY, USA, pp. 26:1–26:27, 2016, February. [20] http://www.taylortjohnson.com/research/johnson2016tecs.pdf

3.B. Publications – Conference Proceedings Papers

- Weiming Xiang, Hoang-Dung Tran, Joel Rosenfeld, Taylor T. Johnson, "Reachable Set Estimation and Verification for a Class of Piecewise Linear Systems with Neural Network Controllers", In American Control Conference (ACC 2018), Special Session on Formal Methods in Controller Synthesis I, IEEE, 2018, June. [39] http://www.taylortjohnson.com/research/xiang2018acc.pdf
- Hoang-Dung Tran, Weiming Xiang, Stanley Bak, Taylor T. Johnson, "Reachability Analysis for One Dimensional Linear Parabolic Equation", In IFAC Conference on Analysis and Design of Hybrid Systems (ADHS 2018), IFAC, 2018, July. [35] http://www.taylortjohnson.com/research/tran2018adhs.pdf
- Shafiul Azam Chowdhury, Soumik Mohian, Sidharth Mehra, Siddhant Gawsane, Taylor T. Johnson, Christoph Csallner, "Automatically Finding Bugs in a Commercial Cyber-Physical System Development Tool Chain With SLforge", In 40th International Conference on Software Engineering (ICSE 2018), ACM, 2018, May. [14] http://www.taylortjohnson.com/research/chowdhury2018icse.pdf
- Andrew Sogokon, Khalil Ghorbhal, Taylor T. Johnson, "Operational models of piecewise-smooth systems", In 17th ACM SIGBED International Conference on Embedded Software (EMSOFT 2017), 2017, October. [32] http://www.taylortjohnson.com/research/sogokon2017emsoft.pdf
- Andrew Sogokon, Khalil Ghorbal, Taylor T. Johnson, "Decoupled simulating abstractions of non-linear ordinary differential equations", Chapter in Proceedings of the 21st International Symposium on Formal Methods (FM 2016), Limassol, Cyprus, 2016, December. [30] http://www.taylortjohnson.com/research/sogokon2016fm.pdf
- Weiming Xiang, Hoang Dung Tran, and Taylor T. Johnson, “Reachable Set Estimation and Control for Switched Linear Systems with Dwell-Time Restriction,” IEEE Conference on Decision and Control [CDC 2016]), December 2016. [37] http://www.taylortjohnson.com/research/xiang2016cdc.pdf
- Parasara Sridhar Duggirala, Chuchu Fan, Matthew Potok, Bolun Qi, Sayan Mitra, Mahesh Viswanathan, Stanley Bak, Sergiy Bogomolov, Taylor T. Johnson, Luan Viet Nguyen, Christian Schilling, Andrew Sogokon, Hoang-Dung Tran, Weiming Xiang, "Tutorial: Software Tools for Hybrid Systems Verification, Transformation, and Synthesis: C2E2, HyST, and TuLiP", In Proceedings of the IEEE Multi-Conference on Systems and Control (MSC 2016), Las Vegas, NV, USA, 2016, September. [19] http://www.taylortjohnson.com/research/duggirala2016msc.pdf
- Muhammad Usama Sardar, Nida Afaq, Khaza Anuarul Hoque, Taylor T. Johnson, Osman Hasan, "Probabilistic Formal Verification of the SATS Concept of Operation", In Proceedings of the 8th NASA Formal Methods (NFM 2016) International Symposium (Sanjai Rayadurgam, Oksana Tkachuk, eds.), Springer International Publishing, pp. 191–205, 2016, June. [29] http://www.taylortjohnson.com/research/sardar2016nfm.pdf
- Stanley Bak, Sergiy Bogomolov, Thomas A. Henzinger, Taylor T. Johnson, Pradyot Prakash, "Scalable Static Hybridization Methods for Analysis of Nonlinear Systems", In 19th Intl. Conf. on Hybrid Systems: Computation and Control (HSCC 2016), ACM, 2016,

April. ***Award for Best Repeatability Evaluation***. [5] http://www.taylortjohnson.com/research/bak2016hscc.pdf

- Stanley Bak, Taylor T. Johnson, "Periodically-Scheduled Controller Analysis using Hybrid Systems Reachability and Continuization", In 36th IEEE Real-Time Systems Symposium (RTSS 2015), IEEE Computer Society, San Antonio, Texas, 2015, December. [7] http://www.taylortjohnson.com/research/bak2015rtss.pdf

3.C. Publications – Workshop Proceedings Papers

- Hoang Dung Tran, Luan Viet Nguyen, and Taylor T. Johnson, "Benchmark: Large-Scale Linear Systems from Order-Reduction," 3rd International Workshop on Applied Verification for Continuous and Hybrid Systems (ARCH 2016), Co-located with CPSWeek 2016, Vienna, Austria, April 2016. [34]
- Andrew Sogokon, Taylor T. Johnson, and Khalil Ghorbal, "Benchmarks for Non-linear Continuous System Safety Verification," 3rd International Workshop on Applied Verification for Continuous and Hybrid Systems (ARCH 2016), Co-located with CPSWeek 2016, Vienna, Austria, April 2016. [31]
- Omar Beg, Ali Davoudi, and Taylor T. Johnson, "Benchmark: Charge Pump Phase-Locked Loops and Full Wave Rectifiers for Reachability Analysis," 3rd International Workshop on Applied Verification for Continuous and Hybrid Systems (ARCH 2016), Co-located with CPSWeek 2016, Vienna, Austria, April 2016. [8]
- Luan Viet Nguyen, Djordje Maksimovic, Taylor T. Johnson, and Andreas Veneris, "Quantified Bounded Model Checking for Rectangular Hybrid Automata," 9th International Workshop on Constraints in Formal Verification (CFV 2015), Co-located with the 34th IEEE/ACM International Conference On Computer Aided Design (ICCAD 2015), November 2015. [27]

3.D. Oral Presentations

- Presented three invited lectures on "Design-Time and Runtime Verification for Safe Autonomous Cyber-Physical Systems," at the Summer School on Cyber-Physical Systems, Halmstad University, Halmstad, Sweden, June 11-15, 2018.
- Presented "SEC Faculty Travel Program Award Presentation: Formal Specification, Verification, & Falsification for Autonomous Cyber-Physical Systems with Hyperproperties & Hybrid Automata," at the Computer Science and Engineering Graduate Seminar (CSCE 681), Texas A&M University, College Station, TX, March 5, 2018.
- Presented paper, "Reachability Analysis for One Dimensional Linear Parabolic Equation," at the IFAC Conference on Analysis and Design of Hybrid Systems (ADHS 2018), Oxford, United Kingdom, July 12, 2018.
- Presented paper, "Benchmark: Continuous-Time Recurrent Neural Networks," at the 5th Applied Verification for Continuous and Hybrid Systems (ARCH 2018), Oxford, United Kingdom, July 13, 2018.
- Presented paper, "Benchmark: Differential Algebraic Equations (DAEs) with Varying Index," at the 5th Applied Verification for Continuous and Hybrid Systems (ARCH 2018), Oxford, United Kingdom, July 13, 2018.
- Presented paper, "Benchmark: Discrete-Space Analysis of Partial Differential Equations," at the 5th Applied Verification for Continuous and Hybrid Systems (ARCH 2018), Oxford, United Kingdom, July 13, 2018.

- Presented "Software Defects in Medical Devices," in conjunction with Prof. Pampee Young's presentation "Software Error in Blood Bank Systems," Vanderbilt University Medical Center (VUMC), Department of Medicine, Division of Hematology and Oncology, Laboratory Medicine Rounds, November 10, 2017.
- Presented "Real-Time Reachability for Safety Verification of Autonomous Cyber-Physical Systems," at the CPS Verification & Validation: Industrial Challenges & Foundations: Safe Implementation of CPS, Carnegie Mellon University, Pittsburgh, PA, May 12, 2017.
- Presented "Real-Time Reachability for Safety of Autonomous Systems," at the Computer Science and Engineering Graduate Seminar (CSCE 681), Texas A&M University, College Station, TX, March 6, 2017.
- Presented "Real-Time Reachability for Verification of Autonomous Cyber-Physical Systems," at the Electrical and Computer Engineering Seminar Series (ECE698/699), Rice University, Houston, TX, March 3, 2017.
- Presented "Real-Time Reachability for Verification of Autonomous Systems," at the Computer Science Seminar, University of Houston, Houston, TX, February 20, 2017.
- Invited Presentation, "Automated Formal Verification for Cyber-Physical Systems," at the Federal Laboratory Day, Laboratory for Telecommunication Sciences, University of Maryland, College Park, MD, March 29, 2016.
- Invited Presentation, "Automated Formal Verification for Cyber-Physical Systems," at the Electrical Engineering and Computer Science Department, Vanderbilt University, Nashville, TN, March 14, 2016.
- Invited Presentation, "Automated Formal Verification for Aerospace Cyber-Physical Systems," at the Aerospace Engineering Department Seminar, University of Michigan, Ann Arbor, MI, March 8, 2016.
- Presented "Automated Formal Verification for Cyber-Physical Systems," at the College of Engineering Advisory Board Meeting, University of Texas at Arlington, Arlington, TX, January 29, 2016.
- Invited Presentation, "Temporal and Functional Correctness in Support of Systems Biology Research," at the Green Center for Systems Biology, University of Texas Southwestern Medical Center at Dallas (UT Southwestern), Dallas, TX, January 13, 2016.
- Invited Presentation, "Automating Verification of Cyber-Physical Systems with HyST," at the Formal Methods Seminar, Department of Computer Science, University of Illinois at Urbana-Champaign, Urbana, IL, December 11, 2015.
- Presented paper, "Quantified Bounded Model Checking for Rectangular Hybrid Automata," at the 9th International Workshop on Constraints in Formal Verification (CFV 2015), Austin, TX, November 5, 2015.
- Invited Presentation, "Real-Time Reachability of Hybrid Systems for Formally Verified Supervisory Control," at the Electrical Engineering Colloquium, University of North Texas, Denton, TX, September 18, 2015.

3.E. Poster and Demo Presentations

- Nathaniel Hamilton and Taylor T. Johnson, "Architecture for an Indoor Distributed Cyber-Physical System Composed of Mobile Robots and Fog Computing Nodes," Poster Session, Safe and Secure Systems and Software Symposium (S5 2017), Dayton, Ohio, August 2017.

- Christina Wang and Taylor T. Johnson, “Moving Target Tracking with Formation Control by Groups of UAVs,” Poster Session, Safe and Secure Systems and Software Symposium (S5 2017), Dayton, Ohio, August 2017.
- Shafiul Chowdhury, Taylor T. Johnson, and Christoph Csallner, “Fuzzing Cyber-Physical System Development Environments With CyFuzz,” Demo Session, 20th International Conference on Hybrid Systems: Computation and Control (HSCC 2017), CPSWeek 2017, Pittsburgh, PA, April 2017.
- Luan Viet Nguyen, James Kapinski, Xiaoqing Jin, Jyotirmoy V. Deskmukh, and Taylor T. Johnson, “Hyperproperties of Real-Valued Signals,” Poster Session, 20th International Conference on Hybrid Systems: Computation and Control (HSCC 2017), CPSWeek 2017, Pittsburgh, PA, April 2017.
- Omar Beg and Taylor T. Johnson, “Computer-Aided Formal Verification for Power Electronics Cyber-Physical systems,” PhD Student Forum, Poster Session, 15th International Conference on Formal Methods in Computer-Aided Design (FMCAD), Austin, TX, September 27-30, 2015.
- Luan Viet Nguyen and Taylor T. Johnson, “Towards Bounded Model Checking for Timed and Hybrid Automata with a Quantified Encoding,” PhD Student Forum, Oral and Poster Sessions, 15th International Conference on Formal Methods in Computer-Aided Design (FMCAD), Austin, TX, September 27-30, 2015.

3.F. PhD Students Supervised

- Luan Viet Nguyen, Computer Science and Engineering, UTA
- Omar Ali Beg, Electrical Engineering, UTA
- Hoang-Dung Tran, EECS, Vanderbilt
- Ayana Wild, EECS, Vanderbilt

3.G. Postdoctoral Research Associates Supervised

- Khaza Hoque, Computer Science and Engineering, UTA
- Andrew Sogokon, EECS Vanderbilt, and Computer Science and Engineering, UTA
- Weiming Xiang, EECS Vanderbilt, and Computer Science and Engineering, UTA
- Joel Rosenfeld, EECS Vanderbilt

3.H. Honors and Awards Received During Period of Award

- Junior Faculty Teaching Fellow, Vanderbilt Center for Teaching, 2018.
- Young Investigator Program (YIP) Award, Air Force Office of Scientific Research (AFOSR), 2016 and 2018.
- Best Software Repeatability Evaluation Award for software artifacts (HyST) developed for publication: Stanley Bak, Sergiy Bogomolov, Thomas A. Henzinger, Taylor T. Johnson, Pradyot Prakash, "Scalable Static Hybridization Methods for Analysis of Nonlinear Systems", In 19th Intl. Conf. on Hybrid Systems: Computation and Control (HSCC 2016), ACM, 2016, April.

3.I. Software Tools and Artifacts

The following software tools and artifacts were developed and improved as a part of this research effort. The tools and examples for the tools are available online.

- HyST: A Source Transformation and Translation Tool for Hybrid Automaton Models
  - http://verivital.com/hyst/
  - https://github.com/verivital/hyst

- Hynger: HYbrid iNvariant GEneratoR: A Dynamic Analysis Tool for Identifying Cyber-Physical Specification Mismatches in Simulink/Stateflow Models
  - http://verivital.com/hynger/
  - https://bitbucket.org/verivital/hynger
- HyRG: Hybrid Random Generator: a software tool for randomly generating hybrid automata for use in differential testing of hybrid systems verification tools
  - http://www.verivital.com/hyrg/

4. References and Bibliography

[1] Ariane 5 flight 501 failure, report by the inquiry board. Technical report, ESA Inquiry Board, Paris, France, July 1996.

[2] Fda medical device recall report 2003 to 2012. Technical report, Food and Drug Administration, March 2014.

[3] H. Alemzadeh, R.K. Iyer, Z. Kalbarczyk, and J. Raman. Analysis of safety-critical computer failures in medical devices. *Security Privacy, IEEE*, 11(4):14–26, 2013.

[4] Stanley Bak, Omar Ali Beg, Sergiy Bogomolov, Taylor T. Johnson, Luan Viet Nguyen, and Christian Schilling. Hybrid automata: from verification to implementation. *Software Tools for Technology Transfer (STTT)*, August 2017.

[5] Stanley Bak, Sergiy Bogomolov, Thomas A. Henzinger, Taylor T. Johnson, and Pradyot Prakash. Scalable static hybridization methods for analysis of nonlinear systems. In *Proc. of the 19th Intl. Conf. on Hybrid Systems: Computation and Control (HSCC)*. ACM, April 2016.

[6] Stanley Bak, Sergiy Bogomolov, and Taylor T. Johnson. HyST: A source transformation and translation tool for hybrid automaton models. In *Proc. of the 18th Intl. Conf. on Hybrid Systems: Computation and Control (HSCC)*. ACM, 2015.

[7] Stanley Bak and Taylor T. Johnson. Periodically-scheduled controller analysis using hybrid systems reachability and continuization. In *36th IEEE Real-Time Systems Symposium (RTSS)*, San Antonio, Texas, December 2015. IEEE Computer Society.

[8] Omar Ali Beg, Ali Davoudi, and Taylor T. Johnson. Charge pump phase-locked loops and full wave rectifiers for reachability analysis (benchmark proposal). In *3rd Applied Verification for Continuous and Hybrid Systems Workshop (ARCH)*, Vienna, Austria, April 2016.

[9] Omar Ali Beg, Luan Viet Nguyen, Taylor T. Johnson, and Ali Davoudi. Signal temporal logic-based attack detection in dc microgrids. *IEEE Transactions on Smart Grids (TSG)*, April 2018.

[10] Boris Beizer. *Software testing techniques (2nd ed.)*. Van Nostrand Reinhold Co., New York, NY, USA, 1990.

[11] M. Broy, I.H. Kruger, A. Pretschner, and C. Salzmann. Engineering automotive software. *Proceedings of the IEEE*, 95(2):356–373, February 2007.

[12] Manfred Broy. Challenges in automotive software engineering. In *Proceedings of the 28th International Conference on Software Engineering*, ICSE '06, pages 33–42, New York, NY, USA, 2006. ACM.

[13] Robert N. Charette. This car runs on code. *IEEE Spectrum*, 2009.

[14] Shafiul Azam Chowdhury. Understanding and improving cyber-physical system models and development tools. In *Proceedings of the 40th International Conference on Software*

Engineering: Companion Proceeedings, ICSE '18, pages 452–453, New York, NY, USA, 2018. ACM.

[15] Consumer Product Safety Commission. Fire alarm control panels recalled by fire-lite alarms due to alert failure (alert #11-702), October 2010.

[16] Consumer Product Safety Commission. Simplex fire alarm control panels recalled by tyco safety products westminster due to failure to alert monitoring centers (alert #11-721), February 2011.

[17] Consumer Product Safety Commission. Fire control panels recalled by bosch security systems corp. due to alarm failure posing a fire hazard (alert #12-721), February 2012.

[18] Mark Dowson. The ariane 5 software failure. *SIGSOFT Softw. Eng. Notes*, 22(2):84, 1997.

[19] Parasara Sridhar Duggirala, Chuchu Fan, Matthew Potok, Bolun Qi, Sayan Mitra, Mahesh Viswanathan, Stanley Bak, Sergiy Bogomolov, Taylor T. Johnson, Luan Viet Nguyen, Christian Schilling, Andrew Sogokon, Hoang-Dung Tran, and Weiming Xiang. Tutorial: Software tools for hybrid systems verification, transformation, and synthesis: C2e2, hyst, and tulip. In *Proceedings of the IEEE Multi-Conference on Systems and Control (MSC 2016)*, Las Vegas, NV, USA, September 2016.

[20] Taylor T. Johnson, Stanley Bak, Marco Caccamo, and Lui Sha. Real-time reachability for verified simplex design. *ACM Transactions on Embedded Computing Systems (TECS)*, February 2016.

[21] Taylor T. Johnson, Stanley Bak, and Steven Drager. Cyber-physical specification mismatch identification with dynamic analysis. In *International Conference on Cyber-Physical Systems (ICCPS)*, 2015.

[22] G. Le Lann. An analysis of the ariane 5 flight 501 failure-a system engineering perspective. In *Engineering of Computer-Based Systems. Proceedings., International Conference and Workshop on*, pages 339–346, 1997.

[23] J. L. Lions. Ariane 5 flight 501 failure. Technical report, Paris, France, July 1996.

[24] National Highway Traffic Safety Administration (NHTSA). (action #pe05029), October 2005.

[25] National Highway Traffic Safety Administration (NHTSA). Honda automatic transmission control module software (recall #11v395000), August 2011.

[26] Luan Viet Nguyen, Khaza Hoque, Stanley Bak, Steven Drager, and Taylor T. Johnson. Cyber-physical specification mismatches. *ACM Transactions on Cyber-Physical Systems (TCPS)*, 2018.

[27] Luan Viet Nguyen, Djordje Maksimovic, Taylor T. Johnson, and Andreas Veneris. Quantified bounded model checking for rectangular hybrid automata. In *9th International Workshop on Constraints in Formal Verification (CFV 2015)*, Austin, Texas, November 2015.

[28] Abbas Saadat. Defect information report (NHTSA Recall 14V-053). February 2014.

[29] Muhammad Usama Sardar, Nida Afaq, Khaza Anuarul Hoque, Taylor T. Johnson, and Osman Hasan. Probabilistic formal verification of the sats concept of operation. In Sanjai Rayadurgam and Oksana Tkachuk, editors, *NASA Formal Methods*, pages 191–205. Springer International Publishing, 2016.

[30] Andrew Sogokon, Khalil Ghorbal, and Taylor T. Johnson. Decoupled simulating abstractions of non-linear ordinary differential equations. In *Proceedings of the 21st*

International Symposium on Formal Methods (FM 2016). Limassol, Cyprus, December 2016.

[31] Andrew Sogokon, Khalil Ghorbal, and Taylor T. Johnson. Non-linear continuous systems for safety verification (benchmark proposal). In *3rd Applied Verification for Continuous and Hybrid Systems Workshop (ARCH)*, Vienna, Austria, April 2016.

[32] Andrew Sogokon, Khalil Ghorbal, and Taylor T. Johnson. Operational models for piecewise-smooth systems. *ACM Trans. Embed. Comput. Syst.*, 16(5s):185:1–185:19, October 2017.

[33] Gregory Tassey. The economic impacts of inadequate infrastructure for software test. Technical Report Planning Report 02-3, National Institute of Standards and Technology, May 2002.

[34] Hoang-Dung Tran, Luan Viet Nguyen, and Taylor T. Johnson. Large-scale linear systems from order-reduction (benchmark proposal). In *3rd Applied Verification for Continuous and Hybrid Systems Workshop (ARCH)*, Vienna, Austria, April 2016.

[35] Hoang-Dung Tran, Weiming Xiang, Stanley Bak, and Taylor T. Johnson. Reachability analysis for one dimensional linear parabolic equations. *IFAC-PapersOnLine*, 51(16):133 – 138, 2018. 6th IFAC Conference on Analysis and Design of Hybrid Systems ADHS 2018.

[36] W. Xiang, D. Tran, and T. T. Johnson. Nonconservative lifted convex conditions for stability of discrete-time switched systems under minimum dwell-time constraint. *IEEE Transactions on Automatic Control*, pages 1–1, 2018.

[37] W. Xiang, H. Tran, and T. T. Johnson. Reachable set estimation and control for switched linear systems with dwell-time restriction. In *55th IEEE Conference on Decision and Control (CDC)*, pages 7246–7251, December 2016.

[38] W. Xiang, H. Tran, and T. T. Johnson. Robust exponential stability and disturbance attenuation for discrete-time switched systems under arbitrary switching. *IEEE Transactions on Automatic Control*, 63(5):1450–1456, May 2018.

[39] W. Xiang, H. Tran, J. A. Rosenfeld, and T. T. Johnson. Reachable set estimation and safety verification for piecewise linear systems with neural network controllers. In *2018 Annual American Control Conference (ACC)*, pages 1574–1579, June 2018.

[40] Weiming Xiang, Hoang-Dung Tran, and Taylor T. Johnson. Output reachable set estimation for switched linear systems and its application in safety verification. *IEEE Transactions on Automatic Control (TAC)*, 2017.

[41] Weiming Xiang, Hoang-Dung Tran, and Taylor T. Johnson. Output reachable set estimation and verification for multi-layer neural networks. *IEEE Transactions on Neural Networks and Learning Systems (TNNLS)*, March 2018.