CURRICULUM VITAE

Updated: April, 2021

Stefano Tonetta

Address
Fondazione Bruno Kessler
via Sommarive, 18
38123 Trento, Italy
Email: stefano.tonetta@fbk.eu

Personal Data
omissis

Academic Qualification

- "Abilitazione Scientifica Nazionale di Seconda Fascia" in "Informatica (01/B1)" and in "Sistemi di Elaborazione delle Informazioni (09/H1)" (April 2017)
- PhD in Information and Communication Technologies (ICT) at the University of Trento (March 2006)
- Laurea in Mathematics (summa cum laude) at the University of Trento (March 2001)

Professional Career

- (04/2021-) Head of the Embedded Systems Unit at Fondazione Bruno Kessler, Trento, Italy.
- (08/2010-) Researcher at Fondazione Bruno Kessler, Trento, Italy.
- (04/2017-) National scientific qualification (Abilitazione Scientifica Nazionale) to function as Associate Professor in the area 09/H1 (Sistemi di Elaborazione delle Informazioni) and 01/B1 (Informatica)
- (08/2007-07/2010) Post-doctoral researcher at the Fondazione Bruno Kessler and responsible of the project "ANACONDA" funded by the Provincia Autonoma of Trento
- (04/2006-07/2007) Post-doctoral researcher at the Faculty of Informatics at the University of Lugano
- (11/2001-03/2006) PhD at the International Graduate School in Information and Communication Technologies (ICT) of the "Università degli Studi di Trento". Thesis: "A new hybrid approach for efficient LTL model checking." Advisor: Prof. Roberto Sebastiani. Co-advisor: Prof. Moshe Y. Vardi.
- (10/2004-10/2004) Stage visiting Rice University at Houston, TX. Supervised by Prof. Moshe Y. Vardi.
- (09/2003-01/2004) Stage visiting Rice University at Houston, TX. Supervised by Prof. Moshe Y. Vardi.
- (09/1996-07/2001) M.S. degree in Mathematics at the University of Trento Final mark: 110/110 cum Laude. Thesis: "Aspetti computazionali della Logica Classica." ("Computational aspects of Classical Logic") Advisor: Prof. Andrea Masini.

Research interests
Formal verification techniques, mainly based on *Model Checking*, their integration in the development process of embedded systems, hardware and software components:

- *Formal methods for requirements validation*: extension of temporal logics with first-order constraints and hybrid aspects, and their satisfiability problem.
- *Verification of hybrid systems*: SMT-based techniques for the verification of network of hybrid systems.

- *Verification modulo theory*: verification techniques for infinite-state transition systems based on SMT: predicate abstraction, bounded model checking, k-induction, interpolation-based.
- *Compositional verification methods*: compositional methods for the verification of complex embedded systems exploiting assume-guarantee reasoning and contract-based specifications.
- *Model-based fault diagnosis and runtime verification*: formal techniques to specify, analyze and synthesize fault diagnoser and runtime monitors.

Publications statistics

- Overall 88 peer-reviewed papers, of which 18 journal papers, 68 conference/workshop papers, 2 book chapters.
- According to Google Scholar: 2234 citations, h-index 25. According to Scopus: 1242, h-index 18.

A full list of publications can be found below.

Service Activities

- Co-Editor of Special Issue on Advances on Computer Safety and Reliability of the Reliability Engineering & System Safety journal, Elsevier 2019, ISSN: 0951-8320
- Co-Editor of Proceedings of Computer Safety, Reliability, and Security - 36th International Conference, SAFECOMP 2017, Trento, Italy, September 13-15, 2017. Lecture Notes in Computer Science 10488, Springer 2017, ISBN 978-3-319-66265-7
- Co-Editor of Proceedings of Computer Safety, Reliability, and Security - SAFECOMP 2017 Workshops, ASSURE, DECSoS, SASSUR, TELERISE, and TIPS, Trento, Italy, September 12, 2017. Lecture Notes in Computer Science 10489, Springer 2017, ISBN 978-3-319-66283-1
- Co-chair and organizer of the 36th International Conference on Computer Safety, Reliability and Security (SAFEOMP17)
- Co-chair and orgnizer of the second SAT/SMT PhD Summer School 2012
- Organizer of tutorial on Model-based design of cyber physical systems at the CSPWeek 2013
- Organizer of AVM 2013, 8th Alpine Verification Meeting
- Organizer of tutorial on Property-Based and Contract-Based Design of System Architectures, co-located with ASE 2013
- Invited speaker at ACVI 2016, workshop on Architecture Centric Virtual Integration
- Invited speaker at CSR 2013, International Workshop on Critical Software Component Reusability and Certification across Domains
- Program Committee member of various international conferences and workshops: SAFECOMP21 (40th International Conference on Computer Safety, Reliability and Security) IJCAI21 (30th International Joint Conference on Artificial Intelligence) AAAI21 (35th AAAI Conference on Artificial Intelligence), IFM20 (16th International Conference on Integrated Formal Methods) RV20 (20th International Conference on Runtime Verification) FMICS20 (25th International Conference on Formal Methods for Industrial Critical Systems) SAFECOMP20 (39th International Conference on Computer Safety, Reliability and Security) IJCAI20 (29th International Joint Conference on Artificial Intelligence) FORMALISE20 (10th International Conference on Formal Methods in Software Engineering) WOSOCER19 (9th IEEE International Workshop on Software Certification), ID-FM19 (Industry Day - Formal Methods 2019), SASSUR19 (Next Generation of System Assurance Approaches for Safety-Critical Systems), SAFECOMP19 (38th International Conference on Computer Safety,

Reliability and Security), FORMALISE19 (9th International Conference on Formal Methods in Software Engineering) RSSRail19 (International Conference Reliability, Safety and Security of Railway Systems), NFM19 (11th NASA Formal Methods Symposium), LATA19 (13th International Conference on Language and Automata Theory and Applications), FM18 (23rd International Symposium on Formal Methods), AI*IA18 PhD Consortium, SASSUR18 (Next Generation of System Assurance Approaches for Safety-Critical Systems), SAFECOMP18 (37th International Conference on Computer Safety, Reliability and Security), S4CIP18 (3rd Workshop on Safety & Security aSSurance for Critical Infrastructures Protection), AAAI18 (32nd AAAI Conference on Artificial Intelligence), DECSOS17 (Dependable Smart Embedded Cyber-physical Systems and Systems-of-Systems) SASSUR17 (Next Generation of System Assurance Approaches for Safety-Critical Systems) S4CIP17 (2nd Workshop on Safety & Security aSSurance for Critical Infrastructures Protection), AAAI17 (31st AAAI Conference on Artificial Intelligence) FM16 Doctoral Symposium, FM16 (21st International Symposium on Formal Methods), SEAA16 (42nd Euromicro Conference on Software Engineering and Advanced Applications), SAFECOMP16 (35th International Conference on Computer Safety, Reliability and Security), NFM16 (8th NASA Formal Methods Symposium), AAAI16 (30th AAAI Conference on Artificial Intelligence) SEAA15 (41st Euromicro Conference on Software Engineering and Advanced Applications), SEAA14 (40th Euromicro Conference on Software Engineering and Advanced Applications), NFM14 (6th NASA Formal Methods Symposium), SEAA13 (39th Euromicro Conference on Software Engineering and Advanced Applications), SEAA12 (38th Euromicro Conference on Software Engineering and Advanced Applications), SEAA11 (37th Euromicro Conference on Software Engineering and Advanced Applications),

- Reviewer for various journals: Springer Journal of Automated Reasoning (2019), Springer journal on Innovations in Systems and Software Engineering (2019), ACM Transactions on Programming Languages and Systems (2018), ACM Transactions on Internet Technology (2016), Journal of the Franklin Institute (2015), Journal of Risk and Reliability (2015), Information and Software Technology (2014), IET Software Journal (2014), Journal of Systems and Software (2014), Theoretical Computer Science (2014), Information Sciences (2013), Journal of Artificial Intelligence Research (2013), Information Sciences (2012), Information and Software Technology (2012), Journal of Applied Logic (2011), Journal of Symbolic Computation (2009), Logical Methods in Computer Science (2007), IEEE Transactions on VLSI Systems (2005)

PhD Faculty Board, Teaching, and Supervising

- Vice-coordinator and Member of Faculty Board of the he Industrial Innovation Doctoral School of the University of Trento.
- Lecturer at the "Sixth Summer School on Formal Techniques" organized by Stanford Research Institute (SRI) from 22-05-2016 to 27-05-2016
- Lecturer of the "Formal Verification of Programs" course at the Doctoral School of the Information and Communication Technologies (ICT) of the University of Trento from 23-02-2009 to 13-03-2009
- Assistant of the "Software Verification" course held by Prof. Natasha Sharygina at the Doctoral School on Information and Communication Technologies (ICT) of the University of Trento from 01-02-2007 to 28-02-2007
- Co-advisor of the PhD student Sergio Mover on "Verification of Hybrid Systems using Satisfiability Modulo Theories" from 01-11-2010 to 31-10-2013

Projects
He participated in several European and internal:

- workpackage leader of HUBCAP (Digital Innovation Hubs and Collaborative Platform for Cyber-Physical Systems), funded by the H2020 program,
- workpackage leader of CITADEL (Critical Infrastructure Protection using Adaptive MILS), funded by the H2020 program,

- task leader of AMASS (Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems) funded by the ECSEL JTI
- workpackage leader of CATSY (Catalogue of System and Software Properties), funded by the European Space Agency
- workpackage leader of D-MILS (Distributed MILS for Dependable Information and Communication Infrastructure"), funded by FP7 program
- workpackage leader of FoReVer (Functional Requirements and Verification Techniques for the Software Reference Architecture), funded by the European Space Agency
- workpackage leader of pSaceCer and nSafeCer (Safety Certification of Software-Intensive Systems with Reusable Components), funded by ARTEMIS JTI
- scientific leader of OthelloPlay funded by Microsoft Software Engineering Innovations Foundation
- responsible for the software project on OCRA
- responsible for the software project on the FBK contributions to CHESS

Full List of Publications

[1] Alberto Griggio, Marco Roveri, and Stefano Tonetta. Certifying proofs for SAT-based model checking. to appear in Formal Methods in System Design.

[2] Alberto Debiasi, Felicien Ihirwe, Pierluigi Pierini, Silvia Mazzini, and Stefano Tonetta. Model-based analysis support for dependable complex systems in CHESS. In Slimane Hammoudi, Luís Ferreira Pires, Edwin Seidewitz, and Richard Soley, editors, *Proceedings of the 9th International Conference on Model-Driven Engineering and Software Development, MODELSWARD 2021, Online Streaming, February 8-10, 2021*, pages 262–269. SCITEPRESS, 2021.

[3] Alessandro Cimatti, Alberto Griggio, Enrico Magnago, Marco Roveri, and Stefano Tonetta. Smt-based satisfiability of first-order LTL with event freezing functions and metric operators. *Inf. Comput.*, 272:104502, 2020.

[4] Alessandro Cimatti, Luca Geatti, Nicola Gigante, Angelo Montanari, and Stefano Tonetta. Reactive synthesis from extended bounded response LTL specifications. In *2020 Formal Methods in Computer Aided Design, FMCAD 2020, Haifa, Israel, September 21-24, 2020*, pages 83–92. IEEE, 2020.

[5] Marco Bozzano, Peter Munk, Markus Schweizer, Stefano Tonetta, and Viktória Vozárová. Model-based safety analysis of mode transitions. In António Casimiro, Frank Ortmeier, Friedemann Bitsch, and Pedro Ferreira, editors, *Computer Safety, Reliability, and Security - 39th International Conference, SAFECOMP 2020, Lisbon, Portugal, September 16-18, 2020, Proceedings*, volume 12234 of *Lecture Notes in Computer Science*, pages 99–114. Springer, 2020.

[6] Peter Gorm Larsen, Hugo Daniel Macedo, John S. Fitzgerald, Holger Pfeifer, Martin Benedikt, Stefano Tonetta, Angelo Marguglio, Sergio Gusmeroli, and George Suciu Jr. A cloud-based collaboration platform for model-based design of cyber-physical systems. In Floriano De Rango, Tuncer I. Ören, and Mohammad S. Obaidat, editors, *Proceedings of the 10th International Conference on Simulation and Modeling Methodologies, Technologies and Applications, SIMULTECH 2020, Lieusaint, Paris, France, July 8-10, 2020*, pages 263–270. ScitePress, 2020.

[7] Alessandro Cimatti, Luca Geatti, Alberto Griggio, Greg Kimberly, and Stefano Tonetta. Safe decomposition of startup requirements: Verification and synthesis. In Armin Biere and David Parker, editors, *Tools and Algorithms for the Construction and Analysis of Systems - 26th International Conference, TACAS 2020, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2020, Dublin, Ireland, April 25-30, 2020, Proceedings, Part I*, volume 12078 of *Lecture Notes in Computer Science*, pages 155–172. Springer, 2020.

[8] Alessandro Cimatti, Alberto Griggio, Enrico Magnago, Marco Roveri, and Stefano Tonetta. Extending nuxmv with timed transition systems and timed temporal properties. In Isil Dillig and Serdar Tasiran, editors, *Computer Aided Verification - 31st International Conference, CAV 2019, New York City, NY, USA, July 15-18, 2019, Proceedings, Part I*, volume 11561 of *Lecture Notes in Computer Science*, pages 376–386. Springer, 2019.

[9] Goran Frehse, Alessandro Abate, Dieky Adzkiya, Anna Becchi, Lei Bu, Alessandro Cimatti, Mirco Giacobbe, Alberto Griggio, Sergio Mover, Muhammad Syifa'ul Mufid, Idriss Riouak, Stefano Tonetta, and Enea Zaffanella. ARCH-COMP19 category report: Hybrid systems with piecewise constant dynamics. In Goran Frehse and Matthias Althoff, editors, *ARCH19. 6th International Workshop on Applied Verification of Continuous and Hybrid Systemsi, part of CPS-IoT Week 2019, Montreal, QC, Canada, April 15, 2019*, volume 61 of *EPiC Series in Computing*, pages 1–13. EasyChair, 2019.

[10] Alessandro Cimatti, Chun Tian, and Stefano Tonetta. Assumption-based runtime verification with partial observability and resets. In Bernd Finkbeiner and Leonardo Mariani, editors, *Runtime Verification - 19th International Conference, RV 2019, Porto, Portugal, October 8-11, 2019, Proceedings*, volume 11757 of *Lecture Notes in Computer Science*, pages 165–184. Springer, 2019.

[11] Alessandro Cimatti, Chun Tian, and Stefano Tonetta. Nurv: A nuxmv extension for runtime verification. In Bernd Finkbeiner and Leonardo Mariani, editors, *Runtime Verification - 19th International Conference, RV 2019, Porto, Portugal, October 8-11, 2019, Proceedings*, volume 11757 of *Lecture Notes in Computer Science*, pages 382–392. Springer, 2019.

[12] Alessandro Cimatti, Rance DeLong, Ivan Stojic, and Stefano Tonetta. Model-based run-time synthesis of architectural configurations for adaptive MILS systems. In Alexander B. Romanovsky, Elena Troubitsyna, and Friedemann Bitsch, editors, *Computer Safety, Reliability, and Security - 38th International Conference, SAFECOMP 2019, Turku, Finland, September 11-13, 2019, Proceedings*, volume 11698 of *Lecture Notes in Computer Science*, pages 200–215. Springer, 2019.

[13] Marco Bozzano, Harold Bruintjes, Alessandro Cimatti, Joost-Pieter Katoen, Thomas Noll, and Stefano Tonetta. COMPASS 3.0. In Tomás Vojnar and Lijun Zhang, editors, *Tools and Algorithms for the Construction and Analysis of Systems - 25th International Conference, TACAS 2019, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2019, Prague, Czech Republic, April 6-11, 2019, Proceedings, Part I*, volume 11427 of *Lecture Notes in Computer Science*, pages 379–385. Springer, 2019.

[14] Alessandro Cimatti, Ramiro Demasi, and Stefano Tonetta. Tightening the contract refinements of a system architecture. *Formal Methods Syst. Des.*, 52(1):88–116, 2018.

[15] Alessandro Cimatti, Ivan Stojic, and Stefano Tonetta. Formal specification and verification of dynamic parametrized architectures. In Klaus Havelund, Jan Peleska, Bill Roscoe, and Erik P. de Vink, editors, *Formal Methods - 22nd International Symposium, FM 2018, Held as Part of the Federated Logic Conference, FloC 2018, Oxford, UK, July 15-17, 2018, Proceedings*, volume 10951 of *Lecture Notes in Computer Science*, pages 625–644. Springer, 2018.

[16] Alberto Griggio, Marco Roveri, and Stefano Tonetta. Certifying proofs for LTL model checking. In Nikolaj Bjørner and Arie Gurfinkel, editors, *2018 Formal Methods in Computer Aided Design, FMCAD 2018, Austin, TX, USA, October 30 - November 2, 2018*, pages 1–9. IEEE, 2018.

[17] Alessandro Cimatti, Rance DeLong, Ivan Stojic, and Stefano Tonetta. Towards adaptive MILS system: Model-based design, verification and run-time adaptation: Slides. In Sergey Tverdyshev, editor, *International Workshop on MILS: Architecture and Assurance for Secure Systems, MILS@DSN 2018, Luxembourg, June 25, 2018*. Zenodo, 2018.

[18] Marco Bozzano, Harold Bruintjes, Alessandro Cimatti, Joost-Pieter Katoen, Thomas Noll, and Stefano Tonetta. Formal methods for aerospace systems. In *Cyber-Physical System Design from an Architecture Analysis Viewpoint*, pages 133–159. Springer, 2017.

[19] Davide Fauri, Daniel Ricardo dos Santos, Elisa Costante, Jerry den Hartog, Sandro Etalle, and Stefano Tonetta. From system specification to anomaly detection (and back). In Bhavani M. Thuraisingham, Rakesh B. Bobba, and Awais Rashid, editors, *Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy, Dallas, TX, USA, November 3, 2017*, pages 13–24. ACM, 2017.

[20] Stefano Tonetta. Linear-time temporal logic with event freezing functions. In Patricia Bouyer, Andrea Orlandini, and Pierluigi San Pietro, editors, *Proceedings Eighth International Symposium on Games, Automata, Logics and Formal Verification, GandALF 2017, Roma, Italy, 20-22 September 2017*, volume 256 of *EPTCS*, pages 195–209, 2017.

[21] Stefano Tonetta, Erwin Schoitsch, and Friedemann Bitsch, editors. *Computer Safety, Reliability, and Security - 36th International Conference, SAFECOMP 2017, Trento, Italy, September 13-15, 2017, Proceedings*, volume 10488 of *Lecture Notes in Computer Science*. Springer, 2017.

[22] Stefano Tonetta, Erwin Schoitsch, and Friedemann Bitsch, editors. *Computer Safety, Reliability, and Security - SAFECOMP 2017 Workshops, ASSURE, DECSoS, SASSUR, TELERISE, and TIPS, Trento, Italy, September 12, 2017, Proceedings*, volume 10489 of *Lecture Notes in Computer Science*. Springer, 2017.

[23] Alessandro Cimatti, Alberto Griggio, Sergio Mover, and Stefano Tonetta. Infinite-state invariant checking with IC3 and predicate abstraction. *Formal Methods Syst. Des.*, 49(3):190–218, 2016.

[24] Alessandro Cimatti, Marco Gario, and Stefano Tonetta. A lazy approach to temporal epistemic logic model checking. In Catholijn M. Jonker, Stacy Marsella, John Thangarajah, and Karl Tuyls, editors, *Proceedings of the 2016 International Conference on Autonomous Agents & Multiagent Systems, Singapore, May 9-13, 2016*, pages 1218–1226. ACM, 2016.

[25] Marco Gario, Alessandro Cimatti, Cristian Mattarei, Stefano Tonetta, and Kristin Yvonne Rozier. Model checking at scale: Automated air traffic control design space exploration. In Swarat Chaudhuri and Azadeh Farzan, editors, *Computer Aided Verification - 28th International Conference, CAV 2016, Toronto, ON, Canada, July 17-23, 2016, Proceedings, Part II*, volume 9780 of *Lecture Notes in Computer Science*, pages 3–22. Springer, 2016.

[26] Jakub Daniel, Alessandro Cimatti, Alberto Griggio, Stefano Tonetta, and Sergio Mover. Infinite-state liveness-to-safety via implicit abstraction and well-founded relations. In Swarat Chaudhuri and Azadeh Farzan, editors, *Computer Aided Verification - 28th International Conference, CAV 2016, Toronto, ON, Canada, July 17-23, 2016, Proceedings, Part I*, volume 9779 of *Lecture Notes in Computer Science*, pages 271–291. Springer, 2016.

[27] Roberto Cavada, Alessandro Cimatti, Luigi Crema, Mattia Roccabruna, and Stefano Tonetta. Model-based design of an energy-system embedded controller using taste. In John S. Fitzgerald, Constance L. Heitmeyer, Stefania Gnesi, and Anna Philippou, editors, *FM 2016: Formal Methods - 21st International Symposium, Limassol, Cyprus, November 9-11, 2016, Proceedings*, volume 9995 of *Lecture Notes in Computer Science*, pages 741–747, 2016.

[28] Christophe Limbrée, Quentin Cappart, Charles Pecheur, and Stefano Tonetta. Verification of railway interlocking - compositional approach with OCRA. In Thierry Lecomte, Ralf Pinger, and Alexander B. Romanovsky, editors, *Reliability, Safety, and Security of Railway Systems. Modelling, Analysis, Verification, and Certification - First International Conference, RSSRail 2016, Paris, France, June 28-30, 2016, Proceedings*, volume 9707 of *Lecture Notes in Computer Science*, pages 134–149. Springer, 2016.

[29] Victor Bos, Harold Bruintjes, and Stefano Tonetta. Catalogue of system and software properties. In Amund Skavhaug, Jérémie Guiochet, and Friedemann Bitsch, editors, *Computer Safety, Reliability, and Security - 35th International Conference, SAFECOMP 2016, Trondheim, Norway, September 21-23, 2016, Proceedings*, volume 9922 of *Lecture Notes in Computer Science*, pages 88–101. Springer, 2016.

[30] Alessandro Cimatti, Ramiro Demasi, and Stefano Tonetta. Tightening a contract refinement. In Rocco De Nicola and eva Kühn, editors, *Software Engineering and Formal Methods - 14th International Conference, SEFM 2016, Held as Part of STAF 2016, Vienna, Austria, July 4-8, 2016, Proceedings*, volume 9763 of *Lecture Notes in Computer Science*, pages 386–402. Springer, 2016.

[31] Marco Bozzano, Alessandro Cimatti, Marco Gario, and Stefano Tonetta. Formal design of asynchronous fault detection and identification components using temporal epistemic logic. *Log. Methods Comput. Sci.*, 11(4), 2015.

[32] Alessandro Cimatti, Marco Roveri, and Stefano Tonetta. HRELTL: A temporal logic for hybrid systems. *Inf. Comput.*, 245:54–71, 2015.

[33] Alessandro Cimatti and Stefano Tonetta. Contracts-refinement proof system for component-based embedded systems. *Sci. Comput. Program.*, 97:333–348, 2015.

[34] Marco Bozzano, Alessandro Cimatti, Oleg Lisagor, Cristian Mattarei, Sergio Mover, Marco Roveri, and Stefano Tonetta. Safety assessment of altarica models via symbolic model checking. *Sci. Comput. Program.*, 98:464–483, 2015.

[35] Marco Bozzano, Alessandro Cimatti, Anthony Fernandes Pires, D. Jones, Greg Kimberly, T. Petri, R. Robinson, and Stefano Tonetta. Formal design and safety analysis of AIR6110 wheel brake system. In Daniel Kroening and Corina S. Pasareanu, editors, *Computer Aided Verification - 27th International Conference, CAV 2015, San Francisco, CA, USA, July 18-24, 2015, Proceedings, Part I*, volume 9206 of *Lecture Notes in Computer Science*, pages 518–535. Springer, 2015.

[36] Cristian Mattarei, Alessandro Cimatti, Marco Gario, Stefano Tonetta, and Kristin Y. Rozier. Comparing different functional allocations in automated air traffic control design. In Roope Kaivola and Thomas Wahl, editors, *Formal Methods in Computer-Aided Design, FMCAD 2015, Austin, Texas, USA, September 27-30, 2015*, pages 112–119. IEEE, 2015.

[37] Harald Rueß and Stefano Tonetta. Distributed MILS (D-MILS) specification, analysis, deployment, and assurance of distributed critical systems. In Sergey Tverdyshev, editor, *International Workshop on MILS: Architecture and Assurance for Secure Systems, MILS@HiPEAC 2015, Amsterdam, The Netherlands, January 20, 2015*. Zenodo, 2015.

[38] Thomas Arts and Stefano Tonetta. Safely using the AUTOSAR end-to-end protection library. In Floor Koornneef and Coen van Gulijk, editors, *Computer Safety, Reliability, and Security - 34th International Conference, SAFECOMP 2015 Delft, The Netherlands, September 23-25, 2015. Proceedings*, volume 9337 of *Lecture Notes in Computer Science*, pages 74–89. Springer, 2015.

[39] Alessandro Cimatti, Rance DeLong, Davide Marcantonio, and Stefano Tonetta. Combining MILS with contract-based design for safety and security requirements. In Floor Koornneef and Coen van Gulijk, editors, *Computer Safety, Reliability, and Security - SAFECOMP 2015 Workshops, ASSURE, DECSoS, ISSE, ReSA4CI, and SASSUR, Delft, The Netherlands, September 22, 2015, Proceedings*, volume 9338 of *Lecture Notes in Computer Science*, pages 264–276. Springer, 2015.

[40] Alessandro Cimatti, Alberto Griggio, Sergio Mover, and Stefano Tonetta. Parameter synthesis with IC3 (informal presentation). In Étienne André and Goran Frehse, editors, *2nd International Workshop on Synthesis of Complex Parameters, SynCoP 2015, April 11, 2015, London, United Kingdom*, volume 44 of *OASICS*, pages 106–107. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2015.

[41] Alessandro Cimatti, Alberto Griggio, Sergio Mover, and Stefano Tonetta. Hycomp: An smt-based model checker for hybrid systems. In Christel Baier and Cesare Tinelli, editors, *Tools and Algorithms for the Construction and Analysis of Systems - 21st International Conference, TACAS 2015, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2015, London, UK, April 11-18, 2015. Proceedings*, volume 9035 of *Lecture Notes in Computer Science*, pages 52–67. Springer, 2015.

[42] Laura Baracchi, Alessandro Cimatti, Gerald Garcia, Silvia Mazzini, Stefano Puri, and Stefano Tonetta. Requirements refinement and component reuse: The forever contract-based approach. In *Handbook of Research on Embedded Systems Design*, pages 209–241. IGI Global, 2014.

[43] Alessandro Cimatti, Sergio Mover, and Stefano Tonetta. Quantifier-free encoding of invariants for hybrid systems. *Formal Methods Syst. Des.*, 45(2):165–188, 2014.

[44] Marco Bozzano, Alessandro Cimatti, Cristian Mattarei, and Stefano Tonetta. Formal safety assessment via contract-based design. In Franck Cassez and Jean-François Raskin, editors, *Automated Technology for Verification and Analysis - 12th International Symposium, ATVA 2014, Sydney, NSW, Australia, November 3-7, 2014, Proceedings*, volume 8837 of *Lecture Notes in Computer Science*, pages 81–97. Springer, 2014.

[45] Roberto Cavada, Alessandro Cimatti, Michele Dorigatti, Alberto Griggio, Alessandro Mariotti, Andrea Micheli, Sergio Mover, Marco Roveri, and Stefano Tonetta. The nuxmv symbolic model checker. In Armin Biere and Roderick Bloem, editors, *Computer Aided Verification - 26th International Conference, CAV 2014, Held as Part of the Vienna Summer of Logic, VSL 2014, Vienna, Austria, July 18-22, 2014. Proceedings*, volume 8559 of *Lecture Notes in Computer Science*, pages 334–342. Springer, 2014.

[46] Alessandro Cimatti, Alberto Griggio, Sergio Mover, and Stefano Tonetta. Verifying LTL properties of hybrid systems with k-liveness. In Armin Biere and Roderick Bloem, editors, *Computer Aided Verification - 26th International Conference, CAV 2014, Held as Part of the Vienna Summer of Logic, VSL 2014, Vienna, Austria, July 18-22, 2014. Proceedings*, volume 8559 of *Lecture Notes in Computer Science*, pages 424–440. Springer, 2014.

[47] Thomas Arts, Michele Dorigatti, and Stefano Tonetta. Making implicit safety requirements explicit - an AUTOSAR safety case. In Andrea Bondavalli and Felicita Di Giandomenico, editors, *Computer Safety, Reliability, and Security - 33rd International Conference, SAFECOMP 2014, Florence, Italy, September 10-12, 2014. Proceedings*, volume 8666 of *Lecture Notes in Computer Science*, pages 81–92. Springer, 2014.

[48] Alessandro Cimatti, Alberto Griggio, Sergio Mover, and Stefano Tonetta. IC3 modulo theories via implicit predicate abstraction. In Erika Ábrahám and Klaus Havelund, editors, *Tools and Algorithms for the Construction and Analysis of Systems - 20th International Conference, TACAS 2014, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2014, Grenoble, France, April 5-13, 2014. Proceedings*, volume 8413 of *Lecture Notes in Computer Science*, pages 46–61. Springer, 2014.

[49] Marco Bozzano, Alessandro Cimatti, Marco Gario, and Stefano Tonetta. Formal design of fault detection and identification components using temporal epistemic logic. In Erika Ábrahám and Klaus Havelund, editors, *Tools and Algorithms for the Construction and Analysis of Systems - 20th International Conference, TACAS 2014, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2014, Grenoble, France, April 5-13, 2014. Proceedings*, volume 8413 of *Lecture Notes in Computer Science*, pages 326–340. Springer, 2014.

[50] Alessandro Cimatti, Sergio Mover, and Stefano Tonetta. Smt-based scenario verification for hybrid systems. *Formal Methods Syst. Des.*, 42(1):46–66, 2013.

[51] Daniel Kroening, Natasha Sharygina, Stefano Tonetta, Aliaksei Tsitovich, and Christoph M. Wintersteiger. Loop summarization using state and transition invariants. *Formal Methods Syst. Des.*, 42(3):221–261, 2013.

[52] Marco Bozzano, Alessandro Cimatti, Marco Gario, and Stefano Tonetta. A formal framework for the specification, verification and synthesis of diagnosers. In *Late-Breaking Developments in the Field of Artificial Intelligence, Bellevue, Washington, USA, July 14-18, 2013*, volume WS-13-17 of *AAAI Workshops*. AAAI, 2013.

[53] Sergio Mover, Alessandro Cimatti, Ashish Tiwari, and Stefano Tonetta. Time-aware relational abstractions for hybrid systems. In Rolf Ernst and Oleg Sokolsky, editors, *Proceedings of the International Conference on Embedded Software, EMSOFT 2013, Montreal, QC, Canada, September 29 - Oct. 4, 2013*, pages 14:1–14:10. IEEE, 2013.

[54] Alessandro Cimatti, Alberto Griggio, Sergio Mover, and Stefano Tonetta. Parameter synthesis with IC3. In *Formal Methods in Computer-Aided Design, FMCAD 2013, Portland, OR, USA, October 20-23, 2013*, pages 165–168. IEEE, 2013.

[55] Alessandro Cimatti, Michele Dorigatti, and Stefano Tonetta. OCRA: A tool for checking the refinement of temporal contracts. In Ewen Denney, Tevfik Bultan, and Andreas Zeller, editors, *2013 28th IEEE/ACM International Conference on Automated Software Engineering, ASE 2013, Silicon Valley, CA, USA, November 11-15, 2013*, pages 702–705. IEEE, 2013.

[56] Natasha Sharygina, Stefano Tonetta, and Aliaksei Tsitovich. An abstraction refinement approach combining precise and approximated techniques. *Int. J. Softw. Tools Technol. Transf.*, 14(1):1–14, 2012.

[57] Alessandro Cimatti, Marco Roveri, Angelo Susi, and Stefano Tonetta. Validation of requirements for hybrid systems: A formal approach. *ACM Trans. Softw. Eng. Methodol.*, 21(4):22:1–22:34, 2012.

[58] Alessandro Cimatti, Sergio Mover, and Stefano Tonetta. Smt-based verification of hybrid systems. In Jörg Hoffmann and Bart Selman, editors, *Proceedings of the Twenty-Sixth AAAI Conference on Artificial Intelligence, July 22-26, 2012, Toronto, Ontario, Canada*. AAAI Press, 2012.

[59] Alessandro Cimatti and Stefano Tonetta. A property-based proof system for contract-based design. In Vittorio Cortellessa, Henry Muccini, and Onur Demirörs, editors, *38th Euromicro Conference on Software Engineering and Advanced Applications, SEAA 2012, Cesme, Izmir, Turkey, September 5-8, 2012*, pages 21–28. IEEE Computer Society, 2012.

[60] Alessandro Cimatti, Sergio Mover, and Stefano Tonetta. A quantifier-free SMT encoding of non-linear hybrid automata. In Gianpiero Cabodi and Satnam Singh, editors, *Formal Methods in Computer-Aided Design, FMCAD 2012, Cambridge, UK, October 22-25, 2012*, pages 187–195. IEEE, 2012.

[61] Marco Bozzano, Alessandro Cimatti, Oleg Lisagor, Cristian Mattarei, Sergio Mover, Marco Roveri, and Stefano Tonetta. Symbolic model checking and safety assessment of altarica models. *Electron. Commun. Eur. Assoc. Softw. Sci. Technol.*, 46, 2011.

[62] Alessandro Cimatti, Marco Roveri, Angelo Susi, and Stefano Tonetta. Formalizing requirements with object models and temporal constraints. *Softw. Syst. Model.*, 10(2):147–160, 2011.

[63] Roberto Sebastiani, Stefano Tonetta, and Moshe Y. Vardi. Symbolic systems, explicit properties: on hybrid approaches for LTL symbolic model checking. *Int. J. Softw. Tools Technol. Transf.*, 13(4):319–335, 2011.

[64] Alessandro Cimatti, Sergio Mover, and Stefano Tonetta. Efficient scenario verification for hybrid automata. In Ganesh Gopalakrishnan and Shaz Qadeer, editors, *Computer Aided Verification - 23rd International Conference, CAV 2011, Snowbird, UT, USA, July 14-20, 2011. Proceedings*, volume 6806 of *Lecture Notes in Computer Science*, pages 317–332. Springer, 2011.

[65] Alessandro Cimatti, Sergio Mover, and Stefano Tonetta. Hydi: A language for symbolic hybrid systems with discrete interaction. In *37th EUROMICRO Conference on Software Engineering and Advanced Applications, SEAA 2011, Oulu, Finland, August 30 - September 2, 2011*, pages 275–278. IEEE Computer Society, 2011.

[66] Alessandro Cimatti, Sergio Mover, and Stefano Tonetta. Proving and explaining the unfeasibility of message sequence charts for hybrid systems. In Per Bjesse and Anna Slobodová, editors, *International Conference on Formal Methods in Computer-Aided Design, FMCAD '11, Austin, TX, USA, October 30 - November 02, 2011*, pages 54–62. FMCAD Inc., 2011.

[67] Roberto Cavada, Alessandro Cimatti, Andrea Micheli, Marco Roveri, Angelo Susi, and Stefano Tonetta. Othelloplay: a plug-in based tool for requirement formalization and validation. In Judith Bishop, Karin K. Breitman, and David Notkin, editors, *Proceedings of the 1st Workshop on Developing Tools as Plug-ins, TOPI 2011, Waikiki, Honolulu, HI, USA, May 28, 2011*, page 59. ACM, 2011.

[68] Daniel Kroening, Natasha Sharygina, Stefano Tonetta, Aliaksei Tsitovich, and Christoph M. Wintersteiger. Loopfrog - loop summarization for static analysis. In Andrei Voronkov, Laura Kovács, and Nikolaj Bjørner, editors, *Second International Workshop on Invariant Generation, WING 2009, York, UK, March 29, 2009 and Third International Workshop on Invariant Generation, WING 2010, Edinburgh, UK, July 21, 2010*, volume 1 of *EPiC Series in Computing*, pages 130–131. EasyChair, 2010.

[69] Lei Bu, Alessandro Cimatti, Xuandong Li, Sergio Mover, and Stefano Tonetta. Model checking of hybrid systems using shallow synchronization. In John Hatcliff and Elena Zucca, editors, *Formal Techniques for Distributed Systems, Joint 12th IFIP WG 6.1 International Conference, FMOODS 2010 and 30th IFIP WG 6.1 International Conference, FORTE 2010, Amsterdam, The Netherlands, June 7-9, 2010. Proceedings*, volume 6117 of *Lecture Notes in Computer Science*, pages 155–169. Springer, 2010.

[70] Angelo Chiappini, Alessandro Cimatti, Luca Macchi, Oscar Rebollo, Marco Roveri, Angelo Susi, Stefano Tonetta, and Berardino Vittorini. Formalization and validation of a subset of the european train control system. In Jeff Kramer, Judith Bishop, Premkumar T. Devanbu, and Sebastián Uchitel, editors, *Proceedings of the 32nd ACM/IEEE International Conference on Software Engineering - Volume 2, ICSE 2010, Cape Town, South Africa, 1-8 May 2010*, pages 109–118. ACM, 2010.

[71] Alessandro Cimatti, Sergio Mover, Marco Roveri, and Stefano Tonetta. From sequential extended regular expressions to NFA with symbolic labels. In Michael Domaratzki and Kai Salomaa, editors, *Implementation and Application of Automata - 15th International Conference, CIAA 2010, Winnipeg, MB, Canada, August 12-15, 2010. Revised Selected Papers*, volume 6482 of *Lecture Notes in Computer Science*, pages 87–94. Springer, 2010.

[72] Alessandro Cimatti, Marco Roveri, and Stefano Tonetta. Requirements validation for hybrid systems. In Ahmed Bouajjani and Oded Maler, editors, *Computer Aided Verification, 21st International Conference, CAV 2009, Grenoble, France, June 26 - July 2, 2009. Proceedings*, volume 5643 of *Lecture Notes in Computer Science*, pages 188–203. Springer, 2009.

[73] Stefano Tonetta. Abstract model checking without computing the abstraction. In Ana Cavalcanti and Dennis Dams, editors, *FM 2009: Formal Methods, Second World Congress, Eindhoven, The Netherlands, November 2-6, 2009. Proceedings*, volume 5850 of *Lecture Notes in Computer Science*, pages 89–105. Springer, 2009.

[74] Roberto Cavada, Alessandro Cimatti, Alessandro Mariotti, Cristian Mattarei, Andrea Micheli, Sergio Mover, Marco Pensallorto, Marco Roveri, Angelo Susi, and Stefano Tonetta. Supporting requirements validation: The eurailcheck tool. In *ASE 2009, 24th IEEE/ACM International Conference on Automated Software Engineering, Auckland, New Zealand, November 16-20, 2009*, pages 665–667. IEEE Computer Society, 2009.

[75] Daniel Kroening, Natasha Sharygina, Stefano Tonetta, Aliaksei Tsitovich, and Christoph M. Wintersteiger. Loopfrog: A static analyzer for ANSI-C programs. In *ASE 2009, 24th IEEE/ACM International Conference on Automated Software Engineering, Auckland, New Zealand, November 16-20, 2009*, pages 668–670. IEEE Computer Society, 2009.

[76] Natasha Sharygina, Stefano Tonetta, and Aliaksei Tsitovich. The synergy of precise and fast abstractions for program verification. In Sung Y. Shin and Sascha Ossowski, editors, *Proceedings of the 2009 ACM Symposium on Applied Computing (SAC), Honolulu, Hawaii, USA, March 9-12, 2009*, pages 566–573. ACM, 2009.

[77] Natasha Sharygina, Stefano Tonetta, and Aliaksei Tsitovich. An abstraction refinement approach combining precise and approximated techniques for efficient program verification: abstract for the invited talk. In *SAVCBS'09, Proceedings of the 8th International Workshop on Specification and Verification of Component-Based Systems, August 25, 2009, Amsterdam, The Netherlands*, pages 35–36. ACM, 2009.

[78] Alessandro Cimatti, Marco Roveri, Angelo Susi, and Stefano Tonetta. Formalization and validation of safety-critical requirements. In Manuela L. Bujorianu and Michael Fisher, editors, *Proceedings FM-09 Workshop on Formal Methods for Aerospace, FMA 2009, Eindhoven, The Netherlands, 3rd November 2009*, volume 20 of *EPTCS*, pages 68–75, 2009.

[79] Alessandro Cimatti, Marco Roveri, and Stefano Tonetta. Symbolic compilation of PSL. *IEEE Trans. Comput. Aided Des. Integr. Circuits Syst.*, 27(10):1737–1750, 2008.

[80] Daniel Kroening, Natasha Sharygina, Stefano Tonetta, Aliaksei Tsitovich, and Christoph M. Wintersteiger. Loop summarization using abstract transformers. In Sung Deok Cha, Jin-Young Choi, Moonzoo Kim, Insup Lee, and Mahesh Viswanathan, editors, *Automated Technology for Verification and Analysis, 6th International Symposium, ATVA 2008, Seoul, Korea, October 20-23, 2008. Proceedings*, volume 5311 of *Lecture Notes in Computer Science*, pages 111–125. Springer, 2008.

[81] Alessandro Cimatti, Marco Roveri, Angelo Susi, and Stefano Tonetta. From informal requirements to property-driven formal validation. In Darren D. Cofer and Alessandro Fantechi, editors, *Formal Methods for Industrial Critical Systems, 13th International Workshop, FMICS 2008, L'Aquila, Italy, September 15-16, 2008, Revised Selected Papers*, volume 5596 of *Lecture Notes in Computer Science*, pages 166–181. Springer, 2008.

[82] Alessandro Cimatti, Marco Roveri, Angelo Susi, and Stefano Tonetta. Object models with temporal constraints. In Antonio Cerone and Stefan Gruner, editors, *Sixth IEEE International Conference on Software Engineering and Formal Methods, SEFM 2008, Cape Town, South Africa, 10-14 November 2008*, pages 249–258. IEEE Computer Society, 2008.

[83] Roberto Sebastiani, Eli Singerman, Stefano Tonetta, and Moshe Y. Vardi. GSTE is partitioned model checking. *Formal Methods Syst. Des.*, 31(2):177–196, 2007.

[84] Alessandro Cimatti, Marco Roveri, Viktor Schuppan, and Stefano Tonetta. Boolean abstraction for temporal logic satisfiability. In Werner Damm and Holger Hermanns, editors, *Computer Aided Verification, 19th International Conference, CAV 2007, Berlin, Germany, July 3-7, 2007, Proceedings*, volume 4590 of *Lecture Notes in Computer Science*, pages 532–546. Springer, 2007.

[85] Roberto Sebastiani, Stefano Tonetta, and Moshe Y. Vardi. Property-driven partitioning for abstraction refinement. In Orna Grumberg and Michael Huth, editors, *Tools and Algorithms for the Construction and Analysis of Systems, 13th International Conference, TACAS 2007, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2007 Braga, Portugal, March 24 - April 1, 2007, Proceedings*, volume 4424 of *Lecture Notes in Computer Science*, pages 389–404. Springer, 2007.

[86] Alessandro Cimatti, Marco Roveri, and Stefano Tonetta. Syntactic optimizations for PSL verification. In Orna Grumberg and Michael Huth, editors, *Tools and Algorithms for the Construction and Analysis of Systems, 13th International Conference, TACAS 2007, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2007 Braga, Portugal, March 24 - April 1, 2007, Proceedings*, volume 4424 of *Lecture Notes in Computer Science*, pages 505–518. Springer, 2007.

[87] Alessandro Cimatti, Marco Roveri, Simone Semprini, and Stefano Tonetta. From PSL to NBA: a modular symbolic encoding. In *Formal Methods in Computer-Aided Design, 6th International Conference, FMCAD 2006, San Jose, California, USA, November 12-16, 2006, Proceedings*, pages 125–133. IEEE Computer Society, 2006.

[88] Roberto Sebastiani, Stefano Tonetta, and Moshe Y. Vardi. Symbolic systems, explicit properties: On hybrid approaches for LTL symbolic model checking. In Kousha Etessami and Sriram K. Rajamani, editors, *Computer Aided Verification, 17th International Conference, CAV 2005, Edinburgh, Scotland, UK, July 6-10, 2005, Proceedings*, volume 3576 of *Lecture Notes in Computer Science*, pages 350–363. Springer, 2005.

[89] Roberto Sebastiani, Eli Singerman, Stefano Tonetta, and Moshe Y. Vardi. GSTE is partitioned model checking. In Rajeev Alur and Doron A. Peled, editors, *Computer Aided Verification, 16th International Conference, CAV 2004, Boston, MA, USA, July 13-17, 2004, Proceedings*, volume 3114 of *Lecture Notes in Computer Science*, pages 229–241. Springer, 2004.

[90] Roberto Sebastiani and Stefano Tonetta. "more deterministic" vs. "smaller" büchi automata for efficient LTL model checking. In Daniel Geist and Enrico Tronci, editors, *Correct Hardware Design and Verification Methods, 12th IFIP WG 10.5 Advanced Research Working Conference, CHARME 2003, L'Aquila, Italy, October 21-24, 2003, Proceedings*, volume 2860 of *Lecture Notes in Computer Science*, pages 126–140. Springer, 2003.

Tesi

- Stefano Tonetta *A new hybrid approach for efficient LTL model checking.* PhD Thesis, March 2006. Contents: the thesis tackles the LTL model checking problem and includes 1) a new approach to LTL compilation and new LTL compiler, 2) a new technique for state-space representation, referred to as *property-driven partitioning* (PDP), based on a hybrid (explicit/symbolic) representation of property automaton and system, 3) an analysis of Generalized Symbolic Trajectory Evaluation, with insights on its relation with model checking algorithms and PDP, 4) a new abstraction technique combining PDP with predicate abstraction, and 5) a deep experimental evaluation.
- Stefano Tonetta *Aspetti computazionali della Logica Classica.* Tesi di Laurea, Luglio 2001. Contents of the thesis: Analysis of some computational aspects of the Classical Logic, such as non-confluence (with a proof of the confluence of Prawitz's system) and expressive power; analysis of the $\lambda\mu$-calculus and of the λ^{Sym}_{Prop}-calculus (with a translation of the former into the latter), both of which encode proofs of Classical Logic.

Awards

- Co-recipient of 2012 FMCAD Best Paper Award
- Co-recipient of FBK 2010 Luigi Stringa award.
- Co-recipient of Microsoft Research SEIF 2010 award.