Cristian Mattarei, PhD

Formal Verification Engineer - Apple Inc.

✉ *cristian.mattarei@gmail.com*
website: mattarei.eu/cristian

Research Interests and Expertise

Symbolic Model Checking, SAT, SMT (Satisfiability Modulo Theories), Formal Modeling, Contract-Based Design, Model-Based Safety Assessment, Safety Assessment, Reliability Analysis.

Professional Experience

Nov. 2018 - present **Formal Verification Engineer**,
Apple Inc., Cupertino, California (USA).
Formal Verification of the Secure Enclave Processor e.g., Apple M1

Oct. 2016 - Nov. 2018 **Postdoctoral Researcher**,
Stanford University, Stanford, California (USA).
Formal Verification of the Javascript Memory Model, and Hardware Model Checking

Nov. 2015 - Oct. 2016 **Researcher**,
Fondazione Bruno Kessler, Trento (Italy).
Symbolic Model Checking Based Safety and Reliability Analysis

Feb. 2014 - Sep. 2014 **Visiting Researcher**,
NASA Ames Research Center, Moffett Field, California (USA).
Formal Verification, Validation, and Safety Analysis of the Functional Allocation project for the NextGen of the Automated Air Traffic Control System

Nov. 2011 - Feb. 2016 **PhD Student/Candidate**,
Fondazione Bruno Kessler, Trento (Italy).
PhD Program in Formal Verification of Safety Critical Systems

Jul. 2010 - Oct. 2011 **Software Engineer**,
Fondazione Bruno Kessler, Trento (Italy).
Design and implementation of the NuSMV integration into the Dassault Aviation OCAS toolset

Jan. 2009 - Aug. 2010 **Software Engineer**,
Fondazione Bruno Kessler, Trento (Italy).
Design and implementation of MathSAT3D: an SMT-based solver for 3D spatial constraints

Mar. 2008 - Mar. 2009 **Formal Modeler**,
Fondazione Bruno Kessler, Trento (Italy).
Formalization and modeling of the European Train Control System (ETCS) interoperability requirements

Education

Feb. 2016 **PhD in Information and Communication Technology**,
University of Trento & Fondazione Bruno Kessler, Trento (Italy).
Thesis: Scalable Safety and Reliability Analysis via Symbolic Model Checking: Theory and Applications. Supervisor: Alessandro Cimatti, Co-supervisor: Marco Bozzano.

Mar. 2011 **Master Degree in Computer Science (Data, Media, and Knowledge)**,
University of Trento, Trento (Italy).

Sep. 2007 **Bachelor Degree in Computer Science**,
University of Trento, Trento (Italy).

Publications

Jan. 2019 **Formal Reliability Analysis of Redundancy Architectures**
M. Bozzano, A. Cimatti, and C. Mattarei*.
FAOC: Formal Aspects of Computing Journal. Vol. 31.

Oct. 2018 **CoSA: Integrated Verification for Agile Hardware Design**
C. Mattarei, M. Mann, C. Barrett, R. G. Daly, D. Huff, and P. Hanrahan.
FMCAD 2018, 18th International Conference on Formal Methods in Computer-Aided Design. Austin, Texas (USA)

Apr. 2018 **EMME: a formal tool for ECMAScript Memory Model Evaluation**
C. Mattarei, C. Barrett, S. Guo, B. Nelson, and B. Smith.
TACAS 2018, 24th International Conference on Tools and Algorithms for the Construction and Analysis of Systems. Thessaloniki (Greece)

Jul. 2016 **Model Checking at Scale: Automated Air Traffic Control Design Space Exploration**
M. Gario, A. Cimatti, C. Mattarei, S. Tonetta, and K. Y. Rozier.
CAV 2016, 28th International Conference on Computer Aided Verification. Toronto (Canada)

Apr. 2016 **The xSAP Safety Analysis Platform**
B. Bittner, M. Bozzano, R. Cavada, A. Cimatti, M. Gario, A. Griggio, C. Mattarei, A. Micheli and G. Zampedri*.
TACAS 2016, 22nd International Conference on Tools and Algorithms for the Construction and Analysis of Systems. Eindhoven (The Netherlands)

Sep. 2015 **Comparing Different Functional Allocations in Automated Air Traffic Control Design**
C. Mattarei, A. Cimatti, M. Gario, S. Tonetta, and K.Y. Rozier.
FMCAD 2015, 15th International Conference on Formal Methods in Computer-Aided Design. Austin, Texas (USA)

Jul. 2015 **Efficient Anytime Techniques for Model-Based Safety Analysis**
M. Bozzano, A. Cimatti, A. Griggio, and C. Mattarei*.
CAV 2015, 27th International Conference on Computer Aided Verification. San Francisco, California (USA)

Nov. 2014 **Formal Safety Assessment via Contract-Based Design**
M. Bozzano, A. Cimatti, C. Mattarei, and S. Tonetta*.
ATVA 2014, 12th International Symposium on Automated Technology for Verification and Analysis. Sydney (Australia)

Jan. 2015 **Safety Assessment of Altarica models via Symbolic Model Checking**
M. Bozzano, A. Cimatti, O. Lisagor, C. Mattarei, S. Mover, M. Roveri, and S. Tonetta*.
SCP: Science of Computer Programming Journal. Vol. 98.

Nov. 2013 **Efficient Analysis of Reliability Architectures via Predicate Abstraction**
M. Bozzano, A. Cimatti, and C. Mattarei*.
HVC 2013, 9th Haifa Verification Conference. Haifa (Israel)

Jul. 2013 **Automated Analysis of Reliability Architectures**
M. Bozzano, A. Cimatti, and C. Mattarei*.
ICECCS 2013, 18th International Conference on Engineering of Complex Computer Systems. Singapore

Sep. 2011 **Symbolic Model Checking and Safety Assessment of Altarica models**
M. Bozzano, A. Cimatti, O. Lisagor, C. Mattarei, S. Mover, M. Roveri, and S. Tonetta*.
AVoCS 2011, 11th International Workshop on Automated Verification of Critical Systems. Newcastle Upon Tyne (United Kingdom)

Nov. 2009 **EuRailCheck: Tool Support for Requirements Validation**
R. Cavada, A. Cimatti, A. Mariotti, C. Mattarei, A. Micheli, A. Susi, S. Mover, M. Pensallorto, M. Roveri, and S. Tonetta*.
ASE 2009, 24th IEEE/ACM International Conference on Automated Software Engineering. Auckland (New Zealand)

**authors in alphabetical order.*

Public Talks

Nov. 30, 2017 **EMME: a formal tool for ECMAScript Memory Model Evaluation**, *Stanford University (USA)*, Stanford, California (USA).

Feb. 10, 2017 **Scalable Safety and Relialibity Analyses via Symbolic Model Checking**, *Stanford University (USA)*, Stanford, California (USA).

Sep. 29, 2015 **Comparing Different Functional Allocations in Automated Air Traffic Control Design**,
FMCAD 2015, 15th International Conference on Formal Methods in Computer-Aided Design, Austin, Texas (USA).

Nov. 4, 2014 **Formal Safety Assessment via Contract-Based Design**,
ATVA 2014, 12th International Symposium on Automated Technology for Verification and Analysis, Sydney (Australia).

Aug. 22, 2014 **Formal Safety Assessment via SAT/SMT**,
Stanford Research International (SRI), Menlo Park, California (USA).

Aug. 11, 2014 **Formal Analysis for Deciding Functional Allocation for AAC: Modeling Approach and Current Results**,
NASA ARC, Flight Trajectory Dynamics and Controls (AFT), Moffett Field, California (USA).

Jun. 23, 2014 **Formal Analysis for Deciding Functional Allocation for AAC: an Overview of the Methodology**,
NASA ARC, Flight Trajectory Dynamics and Controls (AFT), Moffett Field, California (USA).

Nov. 7, 2013 **Efficient Analysis of Reliability Architectures via Predicate Abstraction**,
HVC 2013, 9th Haifa Verification Conference, Haifa (Israel).

Jul. 19, 2013 **Automated Analysis of Reliability Architectures**,
ICECCS 2013, 18th International Conference on Engineering of Complex Computer Systems, Singapore.

May 28, 2013 **Automated Analysis of Reliability Architectures**,
AVM 2013, 8th Alpine Verification Meeting, Trento (Italy).

Sep. 12, 2012 **NuSMV3: a Framework for Model-Based Safety Assessment**,
MBSAW 2012, Model-Based Safety Assessment Workshop, Bordeaux (France).

May 22, 2012 **Library-Based Fault Injection for Formal Safety Assessment**,
AVM 2012, 7th Alpine Verification Meeting, Passau (Germany).

Sep. 12, 2011 **Symbolic Model Checking and Safety Assessment of Altarica models**,
AVoCS 2011, 11th International Workshop on Automated Verification of Critical Systems, Newcastle Upon Tyne (United Kingdom).

Professional Activities

- PC of NFM: NASA Formal Methods Symposium, 2019.
- PC of VaVAS: International Workshop on the Verification and Validation of Autonomous Systems, 2018.
- PC of AAAI: Association for the Advancement of Artificial Intelligence, 2018.
- PC of AAAI: Association for the Advancement of Artificial Intelligence, 2017.
- Peer-reviewer for a total of 18 Journals and International Conferences.

Summer Schools

Jun. 17 - 22, 2013 **13th International School on Formal Methods for the Design of Computer, Communication and Software Systems: Dynamical Systems**,
University Residential Center of Bertinoro, Bertinoro (Italy).

Jun. 12 - 15, 2012 **2nd International SAT/SMT Summer School**,
Fondazione Bruno Kessler, Trento (Italy).

Languages

Italian Native speaker

English Fluent