18th International Conference on Formal Engineering Methods

ICFEM 2016 Final Program

14 ~ 18 November 2016

Welcome to ICFEM 2016

Conference venue

TKP Ichigaya Conference Center (Tokyo, Japan)

Address: 8 Banchi, Ichigayahachimancho, Shinjuku-ku, Tokyo, 162-0844, Japan.

Tel: +81-3-5227-6911

Summary

The ICFEM 2016 program provides three satellite workshops, one tutorial, three keynote talks, one panel discussion, and twenty-seven paper presentations in eight technical sessions. The three workshops are FMMDD 2016, FTSCS 2016, and SOFL+MSVL 2016. FMMDD concentrates on the issues of how to develop trustworthy software-intensive systems using formal methods. FTSCS is concerned with how safety-critical systems can be rigorously developed using formal methods. SOFL+MSVL focuses on all of the development and verification techniques in relation to the practical formal engineering method SOFL or MSVL, or other similar style formal methods. The tutorial introduces the foundations and techniques of CafeOBJ/ProofScores by using elementary examples of natural numbers, sequences, sets and a simple mutual exclusion protocol. The eight technical sessions of the main conference are *Testing/Symbolic Execution*, *Hybrid/Service-Based Systems*, *Security*, *Formal Verification*, *Concurrency/Distributed Systems*, *Model Checking*, *Real-Time Systems*, and *Formal Analysis*.

Co-sponsorships

- The Telecommunications Advancement Foundation (TAF)
- The Murata Science Foundation
- Kayamori Foundation of Informational Science Advancement

In cooperation with

- Hosei University
- The Institute of Electronics, Information and Communication Engineers (IEICE)
- Japan Society for Software Science and Technology (JSSST)

Monday, 14 November 2016	
09:00 ~ 10:00	**Registration (4th Floor, Conference Room 4A)**
FMMDD Workshop (4th Floor, Conference Room 4A)	
10:00 ~ 10:05	**Introduction from the Chairs**
10:05 ~ 11:05	**Invited talk 1** *Stupid Tool Tricks for Smart Model Based Design* Mark Lawford.
11:05 ~ 11:20	**Coffee break**
11:20 ~ 12:50	**Technical talks** *ProRef: An Automatic Authentication Protocol Refinement Tool for Extracting Formal Models* Quanqi Ye, Guangdong Bai, Naipeng Dong and Jin Song Dong. *Modeling Requirements for Quantitative Consistency Analysis and Automatic Test Case Generation* Tom Bienmüller, Tino Teige, Andreas Eggers and Matthias Stasch *Tool Support for Model-Based Database Design with Event-B* Ahmed Al-Brashdi, Michael Butler, Abdolbaghi Rezazadeh and Colin Snook
12:50 ~ 13:50	**Lunch**
13:50 ~ 14:50	**Invited talk 2** *Assured and Correct Dynamic Update of Controllers* Kenji Tei
14:50 ~ 15:50	**Technical talks** *PAndA^2: Analyzing Permission Use and Interplay in Android Apps (Tool Paper)* Manuel Toews, Marie-Christine Jakobs and Felix Pauck. *A Formal Approach to Use Case Driven Testing* Rajiv Murali, Andrew Ireland and Gudmund Grov
15:50 ~ 16:20	**Coffee break**
16:20 ~ 16:50	**Invited industrial presentation** *A trial application of B method for an embedded device by constructing B model via UM* Daichi Mizuguchi.
16:50 ~ 17:40	**Technical talk** *Safety Kernel for Control Systems Design* Alexei Iliasov
17:40 ~ 17:50	**Closing**

FTSCS Workshop (3rd Floor, Conference Room 3D)	
10:00 ~ 10:10	**Opening**
10:10 ~ 11:00	**Specification and verification** *Specification and Verification of Synchronization with Condition Variables* Pedro Gomes, Dilian Gurov and Marieke Huisman *An interval logic for stream-processing functions: A convolution-based construction* Brijesh Dongol
11:00 ~ 11:30	**Coffee break**
11:30 ~ 12:20	**Automotive and railway systems** *Automating Time Series Safety Analysis for Automotive Control Systems in STPA using Weighted Partial Max-SMT* Shuichi Sato, Shogo Hattori, Hiroyuki Seki, Yutaka Inamori and Shoji Yuen *Uniform Modeling of Railway Operations* Eduard Kamburjan and Reiner Hähnle
12:20 ~ 13:30	**Lunch**
13:30 ~ 15:20	**Invited talk + Security, Internet of things** *On Two Higher-Order Extensions of Model Checking* Invited talk: Naoki Kobayashi *Formal Verification of Gate-Level Multiple Side Channel Parameters to detect Hardware Trojans* Imran Abbasi, Faiq Khalid Lodhi, Awais Kamboh and Osman Hasan *Formal Probabilistic Analysis of a WSN-based Monitoring Framework for IoT Applications* Maissa Elleuch, Osman Hasan, Sofiene Tahar and Mohamed Abid
15:20 ~ 15:50	**Coffee break**
15:50 ~ 17:05	**Cyber-physical systems and parameterized verification** *Shared-Variable Concurrency, Continuous Behaviour and Healthiness for Critical Cyberphysical Systems* Richard Banach and Huibiao Zhu *Applying parametric model-checking techniques for reusing real-time critical systems* Baptiste Parquier, Laurent Rioux, Rafik Henia, Romain Soulat, Olivier Roux, Didier Lime and Étienne André Parameterised Verification of Stabilisation Properties via Conditional Spotlight Abstraction Nils Timm and Stefan Gruner
17:05 ~ 17:20	Closing

Tuesday, 15 November 2016	
09:00 ~ 10:00	**Registration (4th Floor, Conference Room 4A)**
SOFL+MSVL Workshop (3rd Floor, Conference Room 3D)	
10:00 ~ 10:10	**Opening**
10:10 ~ 11.00	**Invited talk (Chair: Zhenhua Duan)** *A CEGAR based Approach to Verifying Web Application* Haikou Miao
11:00 ~ 11:30	**Coffee break**
11:30 ~ 12:30	**Session 1 (Chair: Huaikou Miao)** *Formal Development of Linear Structure Reusable Components in PAR Platform* Qimin Hu, Jinyun Xue and Zhen You *The Implementation of MSVL Proof System in Coq* Lin Qian, Zhenhua Duan and Nan Zhang *Orchestration Combinators in Apla+ Language* Zhen You and Jinyun Xue
12:30 ~ 13:30	**Lunch**
13:30 ~ 15:30	**Session 2 (Chair: Jinyun Xue)** *Runtime Verification Monitor Construction for Three-valued PPTL* Xiaobing Wang, Dongmiao Liu, Zhenhua Duan and Liang Zhao *Model Checking of a Mobile Robots Perpetual Exploration Algorithm* Ha Thi Thu Doan, François Bonnet and Kazuhiro Ogata *A Case Study of a GUI-Aided Approach to Constructing Formal Specifications* Fumiko Nagoya and Shaoying Liu *On Termination and Boundedness of Nested Updatable Timed Automata with One Updatable Clock* Yuwei Wang and Guoqiang Li *SMT-based Bounded Model Checking for Cooperative Software with a Deterministic Scheduler* Haitao Zhang and Yonggang Lu *An Automated Solving Procedure for String Function Constraints* Xuzhou Zhang, Ying Xing, Yunzhan Gong, Yawen Wang, Rongyu Liang and Honghui Li.
15:30 ~ 15:55	**Coffee break**
15:55 ~ 17:55	**Session 3 (Chair: Xiaobing Wang)** *Instant-based & State-based Analysis of Infinite Logical Clock* Qingguo Xu, Robert De Simone and Julien Deantoni. *Applying SOFL to a Railway Interlocking System in Industry* Juan Luo, Shaoying Liu, Yanqin Wang and Tingliang Zhou

	A Visual Modeling Language for MSVL Xinfeng Shu, Chao Li, and Chang Liu *E-SSL:An SSL Security-Enhanced Method for Bypassing MITM Attacks in Mobile Internet* Ren Zhao, Xiaohong Li, Guangquan Xu, Zhiyong Feng and Jianye Hao *Automated safety analysis on scenario-based requirements for train control system* Xi Wang *Reliability Testing Data Generation: A Weighted Parameter and Combination Method* Dalin Zhang, Yunzhan Gong, Jianwei Sui and Haitao Zhang
17:55 ~ 18:00	**Closing**

CafeOBJ Tutorial (4th Floor, Conference Room 4A)

Lecturers: Kokichi Futatsugi and Kazuhiro Ogata, JAIST

Overview: CafeOBJ is one of the most advanced algebraic formal specification language systems with a rewriting/reduction engine that can be used for interactive verification. Proof scores are scripts for verification and provide versatile ways to prove properties of specifications. The tutorial gives foundations and techniques of CafeOBJ/ProofScores by using elementary examples of natural numbers, sequences, sets and a simple mutual exclusion protocol.

10:00 ~ 11:00	Proof Scores on Peano Style Natural Numbers
11:00 ~ 11:15	**Coffee break**
11:15 ~ 12:15	Modeling, Specification, and Simulation of Mutual Exclusion Protocol QLOCK
12:15 ~ 14:00	**Lunch**
14:00 ~ 15:00	Proof Score Development for QLOCK with Specification Calculus
15:00 ~ 15:30	**Coffee break**
15:30 ~ 16:30	Formal Verification of Observational Transition Systems with Proof Scores
16:40 ~ 17:40	Formal Verification of Observational Transition Systems with CafeOBJ CITP

Wednesday, 16 November 2016	
08:30 ~ 09:00	**Registration (8th Floor, Banquet Room C)**
09:00 ~ 09:15	**Main Conference Opening (8th Floor, Banquet Room B)**
09:15 ~ 10:15	**Keynote speech (Chair: Shaoying Liu)** *Combinatorial Testing and Its Applications* W. Eric Wong
10:15 ~ 10:45	**Coffee break**
10:45 ~ 12:15	**Testing/Symbolic Execution (Chair: Sungdeok Cha)** *Automated Requirements Validation for ATP Software via Specification Review and Testing* Weikai Miao, Geguang Pu, Yinbo Yao, Ting Su, Danzhu Bao and Yang Liu *Automatic Instance Generation for Validating Alloy Models* Takaya Saeki, Fuyuki Ishikawa and Shinichi Honiden *A General Lattice Model for Merging Symbolic Execution Branches* Dominic Scheurer, Reiner Hähnle and Richard Bubel
12:15 ~ 14:00	**Lunch**
14:00 ~ 16:00	**Hybrid/Service-Based Systems (Chair: Elena Troubitsyna)** *A Case Study of Formal Approach to Dynamically Reconfigurable Systems by Using Dynamic Linear Hybrid Automata* Ryo Yanase, Tatsunori Sakai, Makoto Sakai and Satoshi Yamane *Modelling Hybrid Systems in Event-B and Hybrid Event-B: A Comparison of Water Tanks* Richard Banach and Michael Butler *A System Substitution Mechanism for Hybrid Systems in Event-B* Guillaume Babin, Yamine Ait Ameur, Neeraj Kumar Singh and Marc Pantel *Service Adaptation with Probabilistic Partial Models* Manman Chen, Tian Huat Tan, Jun Sun, Jingyi Wang, Yang Liu, Jing Sun and Jin Song Dong
16:00 ~16:30	**Coffee break**
16:30 ~ 18:00	**Security (Chair: Fatiha Zaidi)** *A Formal Approach to Identifying Security Vulnerabilities in Telecommunication Networks* Linas Laibinis, Elena Troubitsyna, Inna Pereverzeva, Ian Oliver and Silke Holtmanns *Multi-Threaded On-the-fly Model Generation of Malware with Hash Compaction* Minh Hải Nguyễn, Quan Thanh Tho and Le Duc Anh *CPDY: Extending the Dolev-Yao Attacker with Physical-Layer Interactions* Marco Rocchetto and Nils Ole Tippenhauer

Thursday, 17 November 2016	
9:00 ~ 10:00	**Keynote speech (Chair: Mark Lawford) (8th Floor, Banquet Room B)** *A (Proto) Logical Basis for the Notion of a Structured Argument in a Safety Case* Tom Maibaum
10:00 ~ 10:30	**Coffee break**
10:30 ~ 12:30	**Formal Verification (Chair: Toshiaki Aoki)** *Towards the formal verification of data-intensive applications through metric temporal logic* Francesco Marconi, Marcello M. Bersani, Madalina Erascu and Matteo Rossi *Proving Event-B models with reusable generic lemmas* Alexei Iliasov, Alexander Romanovsky and Paulius Stankaitis *Formal Availability Analysis using Theorem Proving* Waqar Ahmed and Osman Hasan *Formal Verification of the rank Algorithm for Succinct Data Structures* Akira Tanaka, Reynald Affeldt and Jacques Garrigue
12:30 ~ 14:00	**Lunch**
14:00 ~ 16:00	**Concurrency/Distributed Systems (Chair: Jin Song Dong)** *Contextual trace refinement for concurrent objects: Safety and progress* Brijesh Dongol and Lindsay Groves *Local Livelock Analysis of Component-Based Models* Madiel Conserva Filho, Marcel Vinicius Medeiros Oliveira, Augusto Sampaio and Ana Cavalcanti *Session-Based Compositional Analysis for Actor-Based Languages Using Futures* Tzu-Chun Chen, Crystal Chang Din and Eduard Kamburjan *An Event-B development process for the distributed BIP framework* Badr Siala, Tahar Bhiri, Jean-Paul Bodeveix and Mamoun Filali-Amine
16:00 ~ 16:20	**Coffee break**
16:20 ~ 17:20	**Panel Discussion (Chair: Shaoying Liu)** *How can formal methods become effective and acceptable "medicine" for software engineering "diseases"?* Panellists: Kokichi Futatsugi, Tom Maibaum, Jin Song Dong, Sungdeok Cha
17:30 ~ 21:30	**Banquet (Symphony Tokyo Bay Dinner Cruise)**

Friday, 18 November 2016	
9:00 ~ 10:00	**Keynote speech (Chair: Kazuhiro Ogata) (8th Floor, Banquet Room B)** *Promotion of Formal Approaches in Japanese Software Industry and a Best Practice of FeliCa's Case* Keijiro Araki
10:00 ~ 10:30	**Coffee break**
10:30 ~ 12:30	**Model Checking (Chair: Cong Tian)** *Partial Order Reduction for State/Event Systems* Shuanglong Kan *Concolic Unbounded-Thread Reachability via Loop Summaries* Peizun Liu and Thomas Wahl *Making Use of Simulation Techniques in Verifying Timed System* Truong Khanh Nguyen, Tian Huat Tan, Jun Sun, Jiaying Li, Yang Liu, Manman Chen and Jin Song Dong *Model Checking Real-Time Properties on the Functional Layer of Autonomous Robots* Mohammed Foughali, Bernard Berthomieu, Silvano Dal Zilio, Félix Ingrand and Anthony Mallet
12:30 ~ 14:00	**Lunch**
14:00 ~ 15:30	**Real-Time Systems (Chair: Richard Banach)** *Decision Problems for Parametric Timed Automata* Étienne André, Didier Lime and Olivier H. Roux *Verifying Nested Lock Priority Inheritance in RTEMS with Java Pathfinder* Saurabh Gadia, Cyrille Valentin Artho and Gedare Bloom *An SMT-based Approach to the Formal Analysis of MARTE/CCSL* Min Zhang, Frederic Mallet and Huibiao Zhu
15:30 ~ 16:00	**Coffee break**
16:00 ~ 17:00	**Formal Analysis (Chair: Shin Nakajima)** *Checking SysML Models for Co-Simulation* Nuno Amalio, Richard Payne, Ana Cavalcanti and Jim Woodcock *A CEGAR Scheme for Information Flow Analysis* Manuel Toews and Heike Wehrheim
17:00 ~ 17:15	**Closing**