GESELLSCHAFT
FÜR INFORMATIK

FoMSESS

GI-Fachgruppe
Formale Methoden
und Software Engineering für sichere Systeme

Herausgeber: Zoltan Mann und Alexander Weigl

Newsletter

6. Ausgabe · Juni 2023

GI-Fachgruppe
Formale Methoden und Software Engineering für sichere Systeme

Newsletter

6. Ausgabe, Juni 2023

Herausgegeben von:

Dr. Zoltán Mann
Informatics Institute
University of Amsterdam
Science Park 900
NL-1098 XH Amsterdam
zoltan.mann@gmail.com

Dr. Alexander Weigl
Institut für Theoretische Informatik
Karlsruhe Institut für Technologie
Am Fasanengarten 5
76131 Karlsruhe
weigl@kit.edu

Vorwort

Liebe Kolleginnen und Kollegen,

Seit der letzten Ausgabe unseres Newsletters im Dezember ist einiges passiert, und noch viel mehr ist in Vorbereitung, wie z.B. das nächste Jahrestreffen der Fachgruppe sowie ein Workshop zur Formalisierung von Gesetzen. Mehr dazu lesen Sie auf den folgenden Seiten.

Sowohl die bisherigen als auch diese Ausgabe des Newsletters sind unter `https://fg-fomsess.gi.de/aktivitaeten/newsletter` zu finden.

Wir wünschen Ihnen einen unbeschwerten Sommer und natürlich viel Spaß bei der Lektüre des Newsletters!

Zoltán Mann
Alexander Weigl

Inhaltsverzeichnis

FoMSESS Jahrestreffen 2023

Auch 2023 findet das FoMSESS-Jahrestreffen **online** statt, am **4. und 5. Oktober**, jeweils **von 15:00 bis 18:00 Uhr**. Merken Sie sich den Termin schon einmal vor!

Die Teilnahme ist kostenlos. Um teilzunehmen, melden Sie sich bitte mit einer formlosen E-Mail an Herrn Zoltan Mann (`zoltan.mann@gmail.com`) an. Geben Sie dabei bitte auch an, ob Sie einen Vortrag halten möchten.

Weitere Informationen werden in Kürze auf folgender Webseite bekanntgegeben:
`https://fg-fomsess.gi.de/veranstaltung/jahrestreffen-2023`

Beitragsaufruf (CfP): Workshop – „Formalisierung von Gesetzen (online)“ der Fachgruppe „Formale Methoden und Software Engineering für sichere Systeme“ (FoMSESS) – *06./07.11.2023 15 Uhr - 18:30 Uhr*

Hintergrund: Die Formalisierung von Gesetzen, wie der DSGVO, kann zur Kontrolle der Einhaltung dieser Gesetze beitragen, indem z.B. datenverarbeitende Systeme automatisch mit der Formalisierung abgeglichen werden. Im vergangenen Workshop FormalDSGVO (2021) haben wir bereits mit Fokus auf der DSGVO über Formalisierungen diskutiert.
Auch in Bereichen wie dem Arbeitsschutz kann eine Formalisierung bei der Kontrolle der Einhaltung helfen. Hierzu müssen allerdings auch alle Maßnahmen und z.B. die Arbeitszeiten so festgehalten werden, dass sie entsprechend mit der Formalisierung abgeglichen werden können. Eine Formalisierung könnte zusätzlich helfen Widersprüche in unterschiedlichen Gesetzen aufzudecken, um dann eine Priorisierung der Gesetze oder eine Auflösung des Wiederspruchs mittels Gesetzesänderung herbeizuführen. Auch in Bezug auf Gesetze zum Umgang mit künstlicher Intelligenz könnten Formalisierungen bei der Einhaltung Unterstützung bieten.

Zielsetzung: Diskussion der Formalisierung von Gesetzen.
Interessante Fragestellungen (nicht vollständig):

- Inwieweit ist eine Formalisierung überhaupt möglich und sinnvoll?
- Welche Hindernisse und Herausforderungen stehen einer Formalisierung im Weg?
- Welche Vorteile kann eine Formalisierung bieten?
- Sollten Gesetze mittels Ontologien formalisiert werden?
- Wie können Juristen mit formalisierten Gesetzen arbeiten?
- Wie können die Formalismen bezüglich Gesetzestreue überprüft werden?

Der Workshop soll die Basis für einen Austausch über aktuelle Forschung und Ideen im Bereich Formalisierung im Kontext von Gesetzen bieten und zur Diskussion über dieses Thema anregen.

Zielgruppe: Der Workshop richtet sich an Interessierte im Bereich formale Methoden und interessierte Juristen

Teilnahme: Gesucht sind Beiträge zum Themengebiet, die in ca. 10 bis 15-minütigen Beiträgen präsentiert und im Anschluss diskutiert werden. Eine Teilnahme ist auch ohne eigenen Beitrag möglich. Gerne können auch neue Ideen, in kürzeren Beiträgen, zur Diskussion präsentiert werden.

Anmeldung/Einreichung: Beiträge sollten in Form eines Abstracts (PDF, max. 2 Seiten) an die Organisatoren angemeldet werden. Die Frist zur Einreichung von Beiträgen ist der **15.10.2023**
Teilnehmer ohne Beitrag können sich noch bis zum Ende des Workshops an Jens Leicht wenden, um Zugang zum Workshop zu erhalten.

Einwahldaten: Der Workshop wird per Zoom abgehalten und die Zugangsdaten per E-Mail versandt.

Organisatoren:

- **Hauptkontakt: Jens Leicht (jens.leicht@uni-due.de)**
- **Mario Gleirscher (mario.gleirscher@uni-bremen.de)**

Fifth Workshop on Formal Methods for Autonomous Systems (FMAS 2023)

FMAS 2023 is a two-day peer-reviewed international workshop that brings together researchers working on a range of techniques for the formal verification of autonomous systems, to present recent work in the area, discuss key challenges, and stimulate collaboration between autonomous systems and formal methods researchers. Previous editions are listed on DBLP: https://dblp.dagstuhl.de/db/conf/fmas/index.html.

More details can be found on our website: https://fmasworkshop.github.io/FMAS2023/

We are applying for a special issue with Science of Computer Programming to accompany FMAS 2023.

Our twitter account is: https://twitter.com/FMASWorkshop and posts about this year's workshop use the tag #FMAS2023

Important Dates

- Submission: 17th August 2023 (Anywhere on Earth https://www.timeanddate.com/time/zones/aoe)
- Notification: 15th September 2023
- Final Version: 20th October 2023
- Workshop: 15th and 16th of November 2023

Scope

Autonomous systems present unique challenges for formal methods. They are often embodied in robotic systems that can interact with the real world, and they make independent decisions. Amongst other categories, they can be viewed as safety-critical, cyber-physical, hybrid, and real-time systems.

Key challenges for applying formal methods to autonomous systems include:

- the system's dynamic deployment environment;
- verifying the system's decision making capabilities -- including planning, ethical, and reconfiguration choices; and
- using formal methods results as evidence given to certification or regulatory organisations.

FMAS welcomes submissions that use formal methods to specify, model, or verify autonomous systems; in whole or in part. We are especially interested in work using integrated formal methods, where multiple (formal or non-formal) methods are combined during the software engineering process. We encourage submissions that are advancing the applicability of formal methods for autonomous systems, for example improving integration or explainability, automation or knowledge transfer of these technique; a wider discussion of these principles can be found in 'A Manifesto for Applicable Formal Methods' https://arxiv.org/abs/2112.12758.

Autonomous systems are often embedded in robotic or cyber-physical systems, and they share many features (and verification challenges) with automated systems. FMAS welcomes submissions with applications to:

7th International Workshop on Security and Privacy Requirements Engineering (SECPRE 2023)

We are glad to announce the SECPRE 2023 7th International Workshop on Security and Privacy Requirements Engineering that will be held in The Hague, The Netherlands, September 28-29, 2023.

SECPRE 2023 (`https://samosweb.aegean.gr/secpre2023/`) will be held in conjunction with the ESORICS 2023 European Symposium on Research in Computer Security (https://esorics2023.org).

SECPRE 2023 proceedings will be published by Springer LNCS Series (post proceedings). Moreover, extended versions of high quality accepted papers will be given fast track opportunity to be published in Information and Computer Security journal (`http://www.emeraldinsight.com/loi/ics`).

SECPRE 2023 is an international, workshop covering research in methods, tools and techniques for the elicitation, analysis and modeling of security and privacy requirements, Security and Privacy testing methods and tools, adaptive Security and Privacy related methods and tools, methods and tools for designing usable secure and privacy-aware systems, methods and tools for the coordination of legal requirements along with Security and Privacy requirements, Security and Privacy requirements verification, integration of functional, security and privacy requirements, Security and Privacy by design issues, Security by design and Privacy by Design legal and regulatory issues.

SECPRE 2023 aims to attract high quality papers in all technical aspects of information security and privacy. Our primary aim is to bring together a critical mass of researchers and practitioners from the academia, industry, and research institutes. We seek unpublished original research or/and technological development contributions, on all theoretical and practical aspects of security and privacy requirements engineering.

Submission deadline: July 03, 2023.

Model-Centric Deductive Verification of Smart Contracts*

Richard Bubel, Reiner Hähnle and Adele Veschetti
{richard.bubel | reiner.haehnle | adele.veschetti}@tu-darmstadt.de

Technische Universität Darmstadt
Software Engineering Group

1 Introduction and Motivation

Establishing trust among different parties without a central agency is the main goal behind distributed ledgers in their most common realization built on blockchain technology.

Smart Contracts are programs that codify real-world transactions and associated protocols (for example, as stated in a legal contract). These programs are stored on the blockchain together with their runtime state between transactions and are executed by the individual nodes. One example of a typical smart contract is an auction application, managing a bidding process. The contract guarantees that the highest bidder wins the auction and the auctioneer receives the money once all conditions are met.

Smart contracts are the ultimate touchstone, codifying the transactions on a blockchain: The *code is law* paradigm is prevalent and strongly promoted. Thus, a central question is: *Do smart contracts correctly implement their intended functionality?* For example, are an auction's rules implemented correctly or are there unintended (or maliciously crafted) code paths permitting to circumvent these rules and thus allowing one of the parties (or an external entity) to take the auctioned item or money without fulfilling their obligations?

Ensuring the correctness of smart contracts is essential for maintaining *trust* in blockchain infrastructures. Blockchains themselves and consensus protocols alone do not cover this aspect. The large number of security vulnerabilities and attacks like the infamous DAO attack, which caused a damage of 50 Million USD worth of Ether, substantiate this claim.

In summary, ensuring trust in the correctness of smart contracts is essential for continued acceptance of distributed ledger technology and its sustainable and responsible usage within society at large. Since the guarantees of blockchains and consensus protocols make it nearly impossible (i.e., very expensive) to adjust erroneous transactions after their completion, it is crucial that the correctness of smart contracts is *ensured before their deployment*.

2 Our Approach

To address this, we propose a methodology that ensures functional correctness and exposes bugs in smart contracts before deployment. Our approach introduces a *modeling language* for smart contracts that permits to describe their intended behavior precisely.

*funded by ATHENE (Nationales Forschungszentrum für angewandte Cybersicherheit)

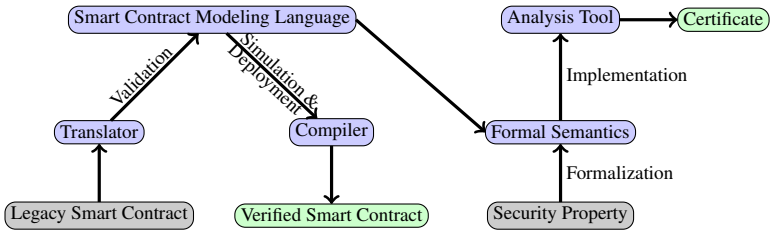

Figure 1: Planned Framework

This model-centric approach offers significant advantages: an easily comprehensible language with a flat learning curve, formal and unambiguous semantics to avoid misunderstandings, and a focus on static verification. By producing correctness certificates based on rigorous proofs, our methodology enhances trust in the correctness of smart contracts.

Furthermore, our approach is *compatible* with existing blockchain technology, because it is possible to translate legacy smart contract languages, such as Solidity, into it.

Problems and Challenges. Figure 1 shows the framework that we develop within the project. The first steps in our projects are focused on (i) the definition of the *Smart Contract Modeling Language* and its *formal semantics*, including (ii) a dynamic type system to ensure that re-entrance (a common source of bugs in smart contracts) is handled safely.

The definition of our modeling language must be performed with great care, because it is central to the success of this project and the foundation for all future tasks. The language must meet the following *main* requirements:

1. Permit clear and *concise* modeling of typical smart contract functionality to permit validation by code inspection
2. Ensure *executability* so that behavior can be simulated as well as models compiled into native code such as the *Ethereum Virtual Machine*
3. Ensure *expressiveness* so that legacy smart contracts can be translated into the modeling language, specifically, to support (nested) programmable transactions
4. Provide a *formal semantics* as the basis for static verification

Afterwards, we continue with the design of a dynamic type system for the modeling language, which guarantees safe re-entrance. The type system infers safety (no re-entrance can happen or it is safe) *statically* for as much of the code as possible and it inserts dynamic checks at code points, where this can neither be proven nor disproven. Thereafter we will develop a logic and calculus to specify and verify complex properties of smart contracts.

In conclusion, we are working on the definition of a language independent modeling framework for smart contracts. By utilizing a high abstraction level inherent in the modeling language, we aim to enhance comprehensibility and facilitate the validation of smart contract behavior. Our proposed modeling language provides concise abstractions for the fundamental concepts underlying various distributed ledger technologies built on blockchains.

At the same time a modeling language permits to abstract away from low-level concerns, which makes it possible to formally prove and certify the absence of several classes of attacks with a high degree of automation.

SFB 1608: “Konsistenz in der sichtenbasierten Entwicklung Cyber-Physikalischer Systeme” bewilligt

Der SFB 1608 “Konsistenz in der sichtenbasierten Entwicklung Cyber-Physikalischer Systeme” wurde erfolgreich von der DFG bewilligt und startet offiziell im Herbst. Die Führung liegt beim KIT und außerdem beteiligt sind die TU München, TU Dresden, Universität Mannheim.

Der SFB erforscht wie Methoden des Software Engineering für den Entwurfs von CPS genutzt und weiterenwickelt werden können. Die zentrale Idee im SFB ist ein gemeinsames virtuelles Metamodell, welches die verschiedenen (Meta-)Modelle während der Entwicklung von CPS abdeckt. Dieses virtuelle Metamodell (virtual single underlying meta model, VSUMM) soll nur in Form von Konsistenzbeziehungen zwischen den einzelnen (Meta-)Modellen, wie CAD-Zeichnungen, SysML, E/E-Architektur oder Programmcode, etabliert werden. Basierend auf dieser Idee gibt es verschiedene formale Ansätze um die Entwicklung mit VSUMM zu ermöglichen. Darunter fallen die Wiederherstellung der Konsistenz durch strukturierte Suche, Verbesserung und Optimierung des Qualitätssicherung von Varianten und Versionen, sowie die Beschleunigung der Typzertifizierung von Fahrzeugen (Homologation) nach Systemänderungen.

www.sfb1608.kit.edu

Stellen: Es sind diverse Doktoranden- und PostDoc-Stellen an den “formalen Lehrstühlen” am KIT (Prof. Beckert, Dr. Ulbrich, Prof. Platzer) verfügbar, aber teilweise noch nicht ausgeschrieben.

Cybersicherheit durch Formale Verifikation

Die formale Verifikation von Soft- und auch Hardware kann einen Beitrag für die Cybersicherheit leisten. Dafür plant die Agentur für Innovation in der Cybersicherheit GmbH (Cyberagentur) in Kürze eine Ausschreibung für Forschungs-Projekte mit Fokus auf einer möglichst durchgängigen Verifikation. Ziel ist ein „Ökosystem vertrauenswürdige IT (ÖvIT)".

Die Cyberagentur mit Sitz in Halle (Saale) beauftragt Forschung zu Cybersicherheitsthemen, die sowohl für die innere und äußere Sicherheit als auch die öffentliche Verwaltung und die Gesellschaft relevant sind.

Auf www.cyberagentur.de/ausschreibungen veröffentlicht sie ihre Ausschreibungen, auch die demnächst zu ÖvIT. Der Newsletter der Cyberagentur, der regelmäßig über Forschungsprojekte und Ausschreibungen informiert, wird über die Veröffentlichung der ÖvIT-Ausschreibung schreiben. Zum Abonnieren reicht eine Mail an newsletter@cyberagentur.de.

Über die Ausschreibung hinaus interessiert die Cyberagentur der direkte Austausch mit Ihnen als FoMSESS-Mitglieder. Wir wollen damit die formale Verifikation in Forschung, Lehre und Anwendung stärken. Möglich ist ein breites Spektrum: gemeinsame Workshops und Veranstaltungen, Kooperationen bei der Betreuung von Bachelor- oder Masterarbeiten oder anderen Projekten. Ansprechpartner ist Dr. Sebastian Jester, Sie erreichen ihn unter oevit@cyberagentur.de

Konferenzkalender

Alle Angaben ohne Gewähr.

iFM 2023: *18th International Conference on integrated Formal Methods*
Erste Frist: 15. Juni 2023 Benachricht.: 10. Aug. 2023 Konferenz: 13.-15. Nov. 2023

SEFM 2023: *21st edition of the International Conference on Software Engineering and Formal Methods*
Erste Frist: 16. Juni 2023 Benachricht.: 18. Aug. 2023 Konferenz: 8.-10. Nov. 2023

GandALF 2023: *Fourteenth International Symposium on Games, Automata, Logics, and Formal Verification*
Erste Frist: 23. Juni 2023 Benachricht.: 7. Aug. 2023 Konferenz: 18.–20. Sept. 2023

ICTAC 2023: *20th International Colloquium on Theoretical Aspects of Computing*
Erste Frist: 25. Juni 2023 Benachricht.: 10. Sept. 2023 Konferenz:
04-08 December 2023

FAACS 2023: *The 7th International Workshop on Formal Approaches for Advanced Computing Systems*
Erste Frist: 30. Juni 2023 Benachricht.: 28. Juli 2023 Konferenz:
18.-19. September, 2023

FTSCS 2023: *9th ACM International Workshop on Formal Techniques for Safety-Critical Systems*
Erste Frist: 12. Juli 2023 Benachricht.: 27. Aug. 2023 Konferenz: 22. Oct. 2023

AREA 2023: *Third Workshop on Agents and Robots for reliable Engineered Autonomy*
Erste Frist: 25. Juli 2023 Benachricht.: 15. August 2023 Konferenz:
30. September - 1. October 2023

FMAS 2023: *Fifth Workshop on Formal Methods for Autonomous Systems*
Erste Frist: 17. Aug. 2023 Benachricht.: 15. Sept. 2023 Konferenz: 15.-16. Nov. 2023

Nächste Ausgabe

Die nächste Ausgabe des Newsletters ist für Dezember 2023 geplant. Der Redaktionsschluss wird voraussichtlich Anfang Dezember 2023 sein. Ein Aufruf zur Einreichung von Beiträgen wird rechtzeitig über die Mailingliste der Fachgruppe FoMSESS verteilt werden.