Praxis der Forschung – Sommersemester 2018

Teilnehmende Arbeitsgruppen im SoSe 2018

- IAR Prof. Asfour, Hochperfomante Humanoide Technologien (H²T)
- ITI Prof. Beckert, Anwendungsorientierte Formale Verifikation
- TM Prof. Beigl, Pervasive Computing Systems (PCS) / TECO
- IAR Prof. Hanebeck, Intelligent Sensor-Actuator-Systems (ISAS)
- IPD Jun.-Prof. Koziolek, Architecture-driven Requirements Engineering (ARE)
- IAR Prof. Kröger, Intelligente Prozessautomation und Robotik (IPR)
- ITI Prof. Müller-Quade, Kryptographie und Sicherheit
- IPD Prof. Reussner, Software Design and Quality (SDQ)
- IPD Prof. Tichy, Programmiersysteme
- TM Prof. Zitterbart, Telematik

Kontakt bei allgemeinen Fragen zu „Praxis der Forschung“:

- Michael Kirsten, ITI Prof. Beckert, kirsten@kit.edu, +49 721 608 45648
- Sarah Grebing, ITI Prof. Beckert, sarah.grebing@kit.edu, +49 721 608 45253
- Erik Pescara, TM Prof. Beigl, pescara@teco.edu, +49 721 608 41704

Termine:

- Anmeldung bis 24.04.2018 bei jeweiligen Betreuern + per Mail bei Michael Kirsten + im ILIAS Kurs **Praxis der Forschung (1. Semester) SoSe 2018**
  https://ilias.studium.kit.edu/goto.php?target=crs_818744
  Bitte Name, Thema und Matrikelnummer bei der Anmeldung angeben.
- **Erste Methodische Veranstaltung:**
  „Kickoff SoSe 2018 und Literaturrecherche“, 26.04.2018, 15:45 - 17:15 Uhr in R. 010, Geb. 50.34

Ausgeschriebene Themen im SoSe 2018

Expertensystem zur Entwicklung humanoider Roboterkomponenten

Die Entwicklung humanoider Roboter ist eine komplexe und zeitintensive Aufgabe. Sie ist stark abhängig von der Erfahrung und dem Expertenwissen einzelner Personen. Um die Entwicklung zukünftiger humanoider Roboter zu unterstützen, ist es wichtig, dieses Expertenwissen zu erhalten. Eine Möglichkeit bietet die Entwicklung eines Expertensystems, einem Programm, das basierend auf einer Wissensbasis wie ein Experte Empfehlungen zur Lösung eines Problems bereitstellt. Für Expertensysteme zur Entwicklung humanoider Roboterkomponenten wurde am H²T bereits eine erste Architektur entwickelt, die aus einer ontologischen Wissensbasis, einer Inferenzmaschine und einer Nutzeroberfläche besteht. Basierend auf technischen Anforderungen des Nutzers wie Länge oder Geschwindigkeit generiert das Expertensystem mögliche Lösungen. Dazu nutzt die Inferenzmaschine die Wissensbasis, in der Katalogkomponenten und Regeln zu deren Verwendung sowie verschiedene strukturelle Optionen zur Anordnung der Teilkomponenten hinterlegt sind. Zur Evaluierung dieser Architektur wurden als Fallstudie Roboter-Gelenkeinheiten gewählt, die aus verschiedenen mechatronischen Teilkomponenten erstellt werden.
Die aktuelle Systemarchitektur ist geeignet um die Entwicklung kleiner Roboterkomponenten zu unterstützen, deren Auswahl auf technischen Anforderungen basiert. Größere humanoide Robotersegmente wie Roboterarme oder Roboterhände haben allerdings oft „High-Level-Anforderungen“, die erst in technische Anforderungen überführt werden müssen. So können beispielsweise ein Arbeitsraum, eine humanoide Kinematik oder sogar konkrete Aufgaben des Roboters „High-Level-Anforderungen“ sein.
Ziel der Arbeit ist es, die existierende Architektur des Expertensystems um Funktionalitäten zu erweitern, damit sie auch für größere Robotersegmente verwendet werden kann. Der Fokus liegt auf dem Überführen von „High-Level-Anforderungen“ in technische Anforderungen, beispielsweise durch Nutzung von Fuzzylogik oder Simulationen. Zur Evaluierung wird ein Expertensystem für ein humanoides Robotersegment wie einen Roboterarm oder eine Roboterhand erstellt. Zur Erstellung der Wissensbasis wird Expertenwissen aus früheren Roboter-Entwicklungen am H²T und aus der Literatur genutzt.
Voraussetzungen für die Durchführung der Arbeit sind fundierte Kenntnisse in C++ oder einer anderen OO-Sprache (z.B. Java, C#). Des Weiteren sollte Interesse an der Entwicklung von Expertensystemen, Kinematik und humanoiden Robotern bestehen.

Kontakt / Betreuung: Samuel Rader (IAR Asfour) samuel.rader@kit.edu

Subsymbolic Prediction of Bimanual Manipulation Action Effects

A robot needs to understand the possible effects of its actions on the environment in order to achieve manipulation goals and avoid undesired side effects. For example, pushing an object on a pile of other objects has the goal of moving the pushed object to a desired pose. However, due to interactions between the pushed object and the pile, other objects might move as well. In a recent work, we used a semantic scene representation consisting of physically plausible support relations between objects to identify possible unsafe actions, which might cause other objects to fall. This work utilizes symbolic preconditions and effects of the executed actions, to detect and handle these situations.
In contrast to symbolic prediction, recent works consider the effects of robot actions on the perceptual level, e.g. a robot perceives its environment through a depth camera and executes a push action. The goal is to predict the perceived depth image after the push action. Subsymbolic prediction has been done on multiple perceptual modalities including camera images, depth images and optical flow. These approaches use deep neural networks to learn the respective prediction models. However, they only consider single actions, like pushing in a specific direction.
We now want to research whether these subsymbolic prediction models can be used for more sophisticated robot actions. In particular, we are interested in bimanual manipulation actions, in which a humanoid robot uses one hand to execute a primary action and the second hand is used to prevent unwanted side effects.

Kontakt / Betreuung: Fabian Paus (IAR Asfour) fabian.paus@kit.edu

Controller Design for Networked Control Systems

Als Networked Control Systems (NCS) werden Regelkreise bezeichnet, bei denen das zu regelnde System räumlich getrennt vom Regler ist, so dass sowohl Sensordaten als auch Stellgrößen über ein weitläufiges Kommunikationsnetz übertragen werden müssen. Klassische Beispiele hierfür sind etwa die Regelung von Satelliten oder anderen unbemannten Raumfahrzeugen. Darüber hinaus sind NCS heutzutage auch für Regelungsaufgaben im Energienetz sowie in Robotik und Automation interessant, da der Einsatz standardisierter Kommunikationsnetze (TCP/IP-basiert, z.B. WLAN, Ethernet) die Flexibilität erhöht und die Wartung vereinfacht. Andererseits bringt die Nutzung von Standard-Netzwerkinfrastruktur und -protokollen auch zusätzliche Herausforderungen für den Entwurf und die Auswahl geeigneter Regelungsalgorithmen mit sich. So müssen Verzögerungen und Paketverluste, aber auch Einschränkungen bzgl. der verfügbaren Bandbreite schon beim Entwurf berücksichtigt werden, um unerwünschte Einflüsse auf die Regelqualität zu vermeiden. Eine Konsequenz daraus ist, dass der Regler dann nicht exakt weiß, wann eine versendete Stellgröße tatsächlich genutzt wird. Diese Information ist aber für eine akkurate Prädiktion des Systemverhalten notwendig, welche üblicherweise wiederum für die Berechnung zukünftiger Stellgrößen benötigt wird.
Abhilfe hierfür schafft das selektive Versenden von Quittungen auf Anwendungsebene. In den meisten existierenden Ansätzen in der Literatur wird jedoch angenommen, dass solche Quittungen verlustfrei und ohne Verzögerungen übertragen werden können, was eine starke Einschränkung darstellt. Im Rahmen dieses Projekts soll daher, aufbauend auf Vorarbeiten am ISAS, ein Regelungsalgorithmus entworfen werden, der berücksichtigt, dass Quittungen auch verloren gehen können bzw. erst verspätet eintreffen.

Kontakt / Betreuung: Florian Rosenthal (IAR Hanebeck) florian.rosenthal@kit.edu

HoloBike: Entwurf und Umsetzung eines Radfahr-Simulators für virtuelle Realitäten

Am Lehrstuhl für intelligente Sensor-Aktor-Systeme (ISAS) wird seit 15 Jahren Telepräsenz betrieben. Dabei wurde zuerst mit Hilfe von Tracking-Verfahren und Virtual-Reality(VR)-Brillen eine Immersion des Benutzers in eine virtuelle Umgebung sowie mit Hilfe eines Roboter-Avatars eine Immersion in entfernte reale Umgebungen ermöglicht. Durch das am Lehrstuhl entwickelte Verfahren der Bewegungskompression kann der Benutzer in der entfernten Umgebung weite Strecken zurücklegen, welche mit einer direkten Übertragung nicht in das Arbeitsfeld des Benutzers passen würden. Dieses System wurde vor kurzem durch einen Fahrsimulator erweitert, wobei hier als nächster Schritt sogenannte ”virtual shared spaces“ erstellt werden. Dabei sollen sich lokale, wie auch entfernte virtuelle Fußgänger sowie Autofahrer in einer gemeinsamen virtuellen Umgebung bewegen, miteinander und mit der Umgebung interagieren können.
Das vorliegende Forschungsprojekt hat als Zielsetzung, unser VR-Labor (”Holodeck“) um einen VR-Radfahr-Simulator (”HoloBike“) zu erweitern. Dies beinhaltet den kompletten Entwicklungsprozess von der Anforderungsanalyse, über den Aufbau des Radfahr-Simulators bis hin zur späteren Verbindung mit unserem vorhandenen VR-System.

Kontakt / Betreuung: Christian Tesch (IAR Hanebeck) tesch@kit.edu

Localization of a Robotic Platform using ARCore

In the last few years, visual odometry has made large strides both in robustness and resource efficiency. The idea in this field is to allow for the real-time localization of a camera by finding certain markers or features in a video image, and then estimating their three-dimensional position in the world. Then, by following their motion in successive frames, it is possible to obtain the position and orientation of the camera accurately, without requiring additional hardware or changes in the infrastructure. The entrance of giants such as Google and Apple in the last few months has further revolutionized the field, allowing for visual odometry to be usable even in small devices such as smartphones. While their main target is the field of augmented reality, the tracking algorithms can also be used in many other applications.

In this project, we want to explore the applicability of Google's ARCore for use in robotic indoor localization and navigation. The idea is to attach a smartphone on a small moving robotic platform, called *Omnimover*, to allow it to locate itself as it carries a load to a given location. This task is not straightforward, as the robot needs to know its absolute starting position, avoid sensor drift, detect and move around obstacles, and solve many other issues. Robustness must also be taken into account, given that the robot needs to work in a large variety of scenarios and environments.

Kontakt / Betreuung: Antonio Zea (IAR Hanebeck) antonio.zea@kit.edu

Sensoreinsatzplanung in der Schüttgutsortierung

Bei sogenannten optischen Bandsortieranlagen werden Teilchen auf Basis visueller Eigenschaften separiert. Bei der Anlage, so wie sie bei Kunden des Fraunhofer IOSB im Einsatz ist, werden Teilchen einer Klasse von Teilchen einer anderen Klasse getrennt. Durch richtiges Timing und gezieltes Aktivieren von Druckluftdüsen wird eine Klasse von Teilchen während einer nach der Bandkante beginnenden Flugphase ausgeblasen. Aufgrund von Verzögerungen ist es nicht möglich, die Klassifikation und die Separation gleichzeitig zu vollziehen, weshalb die Position der Teilchen nach ihrer Detektion und Klassifikation vorhergesagt werden muss.
Um akkurate Prädiktionen zu ermöglichen, haben wir kürzlich vorgeschlagen, die Teilchen auf dem Band mit einer Flächenkamera zu beobachten und so deren Trajektorien zu rekonstruieren. Dies geschieht mit Techniken des Multitarget Trackings. Da die Algorithmen der Bildverarbeitung und des Multitarget Trackings viel Rechenzeit benötigen, können die Algorithmen nicht mit aktuellen Hochgeschwindigkeitskameras, die mehr als 300 Frames pro Sekunde ermöglichen, mithalten. In diesem Projekt soll ein Regler entworfen werden, der eine Teilmenge der Bilddaten bestimmt, mit der unter Berücksichtigung der Echtzeitfähigkeit die Genauigkeit der Vorhersagen maximiert wird. Die Algorithmen zum Tracking und der Bildverarbeitung existieren bereits und dürfen dabei als unveränderlich angenommen werden.

Kontakt / Betreuung: Florian Pfaff (IAR Hanebeck) florian.pfaff@kit.edu
Jana Mayer (IAR Hanebeck) jana.mayer@kit.edu
Dr. Benjamin Noack (IAR Hanebeck) benjamin.noack@kit.edu

Simultaneous Localization and Mapping based on Directional Estimation

Simultaneous Localization and Mapping (SLAM) denotes the technique of constructing or updating a map of unknown surroundings (*mapping*) while at the same time estimating an agent's pose (*tracking*). It plays a central role in a variety of application scenarios, such as autonomous driving, robotic perception, manipulation as well as navigation in unknown environments. However, due to the high nonlinearity and dynamics of rigid body motions, which mathematically belong to the *special Euclidean group SE*(3), the tracking step is still challenging in real-world scenarios. Conventional pose estimation methods include applying the stochastic filters, e.g., from the well-known Kalman filter family, or the Monte Carlo-based particle filters, which lack the necessary probabilistic interpretation of the nonlinearity underlying the manifold of *SE*(3). In some vision-based scenarios numerical approaches are also applied but they typically have the assumption of small motion between consecutive frames.
Directional statistics, a subfield of statistics, specifically deals with uncertain directional variables on nonlinear manifolds such as *SE*(2), *SE*(3), *SO*(3), etc.. Distributions from this subject have been further applied to construct some *directional estimation* approaches for tracking. In this project, a novel pose estimator will be implemented for performing SLAM in real-world scenarios and further get evaluated under challenging circumstances.

Kontakt / Betreuung: Kailai Li (IAR Hanebeck) kailai.li@kit.edu

Reinforcement Learning for Behaviour from Similarity of Visual Output

Im Bereich der Medizinrobotik sind lernende Systeme, die physisch mit ihrer Umgebung interagieren, mit untragbar großen Risiken verbunden. Ein System, das sich noch nicht optimal und sicher verhält, darf nicht in Kontakt mit Patienten kommen. Lernen in der Simulation ist daher von großer Bedeutung, da dort aus Fehlern gelernt werden kann, die in der Realität zu schwere Folgen hätten.
Fokus dieser Arbeit soll ein Kameraroboter sein, der eine Szene überwachen soll und seine Position so verändert, dass relevante Teile der Szene immer sichtbar sind. Oft ist es der Fall, dass diese Aufgabe durch Telemanipulation des Roboters durch einen Menschen gut lösbar, aber schwer formalisierbar und damit schwer automatisierbar ist. Moderne Methoden des Deep Reinforcement Learning stellen hierbei einen vielversprechenden Lösungsansatz dar.
Nachdem zunächst in einer Simulation ein Szenario einer Szenenüberwachung implementiert wird, soll das System so designt werden, dass ein Mensch per Telemanipulation das Szenario durchspielen kann und sowohl seine Steuersignale als auch der visuelle Output aufgezeichnet wird.
In einem zweiten Schritt soll ein Agent das Szenario durchspielen und anhand eines Rewards sein Verhalten so ändern, dass es dem Verhalten des Menschen angenähert wird. Hierdurch soll das Verhalten eines Menschen gelernt werden, ohne es explizit formalisieren zu müssen. Der Reward soll sich daran orientieren wie ähnlich die visuellen Outputs des Agenten den visuellen Outputs des Menschen sind (hierbei kann die Bewertung des Bildes sowohl auf Pixel- als auch auf symbolischer Ebene durch eine Vorverarbeitung geschehen, z. B. Durch semantische Segmentierung). Die Steuersignale können nachfolgend zur Evaluation genutzt werden.
Als konkreter Anwendungsfall soll ein Szenario im Operationssaal umgesetzt werden, bei dem eine Kamera den Kopf des Patienten dauerhaft beobachten soll. Die Bewegung der Kamera soll hierdurch Verdeckungen verhindern, wenn sich z. B. der Chirurg zwischen Kamera und Kopf stellt.

Kontakt / Betreuung: Paul Maria Scheikl (IAR Kröger) paul.scheikl@kit.edu

Abbildung natürlicher Sprache auf bestehende Modellstrukturen

(Thema bereits vergeben.)

Kontakt / Betreuung: Tobias Hey (IPD Tichy) hey@kit.edu
Jan Keim (IPD Koziolek) jan.keim@kit.edu
Jun.-Prof. Anne Koziolek (IPD Koziolek) anne.koziolek@kit.edu

Erforschung modularer Simulationskonzepte im Rahmen von Cyber-physischen Systemen

Um das Verhalten eines Systems analysieren zu können, stehen unterschiedliche Verfahren zur Auswahl. Zum einen ist es möglich, dass zu analysierende System mit der gewünschten Konfiguration umzusetzen. Zum anderen kann das System mithilfe einer Simulation auf gewünschte Eigenschaften untersucht werden. Der zweite Fall kommt immer mehr zum Einsatz, gerade wenn die Kosten oder der Aufwand die Realisierung unmöglich machen. Ebenso kann die Modularisierung von Simulationen dazu beitragen, die Kosten für die Entwicklung zu reduzieren, indem Teilelemente wiederverwendet werden können.

Kontakt / Betreuung: Sandro Koch (IPD Reussner) sandro.koch@kit.edu

Impact-Analyse von Angriffen auf Industrie 4.0 Systeme

Industrie 4.0-Umgebungen und andere IoT-Umgebungen bestehen in der Regel aus vielen verschiedenen Komponenten/Akteuren. Diese tauschen häufig Daten aus und bilden damit ein komplexes, unübersichtliches Datennetz. Gerade im Fall eines Angriffs/Einbruch ist es jedoch nötig, schnell abzuschätzen, welche Daten betroffen sein können. Firmen und Institutionen können jedoch aufgrund mangelhafter Dokumentation und Analysetechniken häufig kaum feststellen, welche Daten konkret betroffen sind, oder benötigen hierfür sehr lange. Um eine bessere Übersicht über den Datenaustausch der verschiedenen Komponenten zu erreichen, kann dieser als Datenfluss in ein einem Architekturmodell erfasst werden. Basierend auf der Datenflussmodellierung kann dann mittels Ausbreitungsanalysen abgeschätzt werden, welche Daten ein Angreifer in einem System sehen konnte und damit stehlen oder korrumpieren konnte.
Zuerst sollen typische Angriffsszenarios (Einbruch und Ausbreitung in Systemen) für Industrie 4.0-Umgebungen recherchiert werden. Eine Auswahl dieser Angriffsszenarien soll anschließend in einem Angreifermodell (Einstiegspunkt und Ausbreitungsregeln) für die gegebenen Datenflussarchitektur modelliert werden. Eine prototypische Umsetzung der Ausbreitungsanalyse ist ebenfalls geplant. Als Grundlage steht die Datenflussmodellierung von Palladio zur Verfügung.

Kontakt / Betreuung:	Maximilian Walter (IPD Reussner)	maximilian.walter@kit.edu
	Stephan Seifermann (IPD Reussner)	stephan.seifermann@kit.edu

Bislicing – Slicing for Relational Verification

The problem whether two programs are equivalent is of great interest in the daily practice of software development—especially in order to support evolving software systems. We developed reve, a tool that proves the equivalence of two C programs with the same behaviour on a local function level. This leads to the next challenge: the scalability on full software projects.
Lightweight analysis techniques provide *Program Dependence Graphs* (PDGs) that capture all dependencies between statements within one program. We can use the well-known theoretical result that two equivalent programs have isomorphic PDGs in order to rapidly check whether certain parts of the two analyzed programs are equivalent. This would allow reve to focus on the more difficult program parts. We call this process of excluding equivalent parts (this result is taken from the PDG-analysis) of the two programs for the equivalence verification *bi-slicing*.
The focus of this thesis should be a theoretical concept of bi-slicing for case equivalence checking. Implementation and evaluation are also on the agenda, but subordinate.

Kontakt/Betreuung:	Mihai Herda (ITI Beckert)	herda@kit.edu
	Dr. Mattias Ulbrich (ITI Beckert)	ulbrich@kit.edu

Hyper Test Tables

Hyper properties became very popular in the last years, because of their expressive power. The core of hyper properties is the possibility to (uni-versal and existential) quantified over program traces. For example, this enables the specification of refinement (“forall runs in the old software revision, exists a run in the new revision“) or:
“Hyperproperties can express security policies, such as secure information flow and service level agreements, that trace properties cannot.“ (Clarkson and Schneider in Hyperproperties. JCS 18. 2010.)
The goal is a table-based specification language, that (a) supports hyper properties and (b) is decidable by state-of-the-art tools (model checker or SMT solver).
Your task is to understand the current work of generalized test tables, HyperLTL and HyperCTL. You define the syntax and sematic of the specification language and implement a decision procedure for proving the conformance of reactive system to your specification.

Kontakt/Betreuung:	Alexander Weigl (ITI Beckert)	weigl@kit.edu

Inferring JML Contracts for KeY from System Dependence Graphs

Die beiden am KIT entwickelten Tools JOANA und KeY erlauben die statische Analyse von Java-Programmen. Ziel von JOANA ist es, die Noninterference-Eigenschaft (d. h. öffentliche Ausgaben werden von geheimen Eingaben nicht beeinflusst) von einem Programm nachzuweisen. Die Analyse von JOANA findet rein syntaktisch mit Hilfe von Systemabhängigkeitsgraphen (SDGs) statt. Das erlaubt voll automatisierte und schnelle Analysen; Programme mit bis zu 100k Zeilen Code können analysiert werden. KeY wiederum ist ein Theorembeweiser, der zwar allgemeinere Eigenschaften von Programmen verifizieren kann, aber deutlich weniger skaliert als JOANA.
Das Ziel diese Projekts ist es, die hochskalierbaren SDG-basierten Ansätze, auf denen JOANA beruht, für die Inferenz korrekter Programmeigenschaften zu verwenden. Diese Eigenschaften (z. B. Lese- und Schreibzugriffe einer Methode, Informationsflussverträge, u. a.) sollen in Form von Programmspezifikationen erzeugt werden.

Kontakt/Betreuung: Mihai Herda (ITI Beckert) herda@kit.edu

Ownership Types and Dynamic Frames

Formal program verification is a powerful technology to ensure that a program's effects are as desired. However, formal verification can be quite a challenging endeavour. One of the major challenge is the so called *Frame Problem*: showing that a program does not affect certain parts of the memory.
The goal of the work in this thesis is to bring two successful solutions for the frame problem together: Combine (1) *Ownership Types* and (2) *Dynamic Frames* for Convenient and Flexible Framing Specifications. The former scales very well while the latter is very general and precise. We want to combine the benefits of both paradigms to obtain a very flexible frame specification technology.
Your task is to integrate the framing technology of Dynamic Frames for JML (as implemented in our verification tool KeY) with an ownership type system defined in the Java Checker Framework.

Kontakt/Betreuung: Mattias Ulbrich (ITI Beckert) ulbrich@kit.edu

Property-Directed Reachability for Regression Verification

Since 2007, IC3 and property-directed reachability (PDR) became de-facto standard in the domain of symbolic model checking. Both approaches are decision procedures to verify that a given invariant holds for the modelled system. With Regression Verification, we can prove that two given systems with the same behaviour are functionally equivalent (minus the intended changes). In our case we apply Regression Verification in the field of automated production systems to ensure the well-functioning during software evolution.
The goal of this thesis is the transfer of current PDR/IC3 approaches to software model checking in order to outperform current regression verification implementations. The idea is to exploit the main assumption behind regression verification, which is that both software versions have a high degree of similar structures. As a benchmark scenario we use the Pick-and-Place-Unit from TUM.
Your task is to understand the current State-of-the-Art of PDR and IC3; adapt the ideas into a novel approach, and perform the benchmarks.

Kontakt/Betreuung: Alexander Weigl (ITI Beckert) weigl@kit.edu

Property-Oriented Component Library for Voting Rules

Voting rules are algorithms to aggregate multiple individual decisions (e.g., for electing a parliament) into one election outcome. They aim to establish trust in an election process by balancing a variety of desiderata such as, e.g., proportionality and majority representation. Most voting rules are designed to satisfy many of them, but experiences show that errors are easy to make, see e.g., the changed German federal elections 2013 to comply with the German constitution. Social choice theory defined many such requirements in "axiomatic properties".

The goal of this work is to identify and analyse voting rules for core components, e.g., some elimination mechanism in a round-based voting rule, or some mechanism to resolve ties between candidates, etc, which enable a property-oriented construction of voting rules. The resulting component library should enable the user to construct her own voting rule, knowing that already some specified properties are guaranteed by the underlying components. The vision of this library is to support the development of voting rules which guarantee a high level of trust by construction without the need to re-check the whole voting rule.

Kontakt / Betreuung: Michael Kirsten (ITI Beckert) kirsten@kit.edu

Relational Debugging for Scalable Algorithms

In contrast to functional properties, relational properties are universally quantified over multiple program runs. This allows the specification of complex properties. For example: (1) the absence of information flow from confidential input to public output, (2) the equivalence of two programs under the same input, or (3) the numerical stability in scalable algorithms with floating points. If a relational property is violated, the developer needs investigation tools to find the reason. For functional properties, the tools of choice are debuggers, that allow a coarse or fine-grained stepping through a program run and inspection of the internal variable assignments. For relational properties, the developer needs to be able to step through multiple program runs simultaneously.
The goal of this thesis is to develop a full-featured debugger for relational properties applicable for *real* programming languages and *real-sized* software! We need to develop and deploy several features to handle the increased complexity of simultaneously debugging, like relational synchronization points, relational invariants, or user annotations. Your task is to develop a relational debugger. This includes concepts of (1) embedding of user annotation and specification, (2) integration of (semi-)formal methods to aid the user, (3) visualization and user interaction. This project should result into a working prototype.

Kontakt/Betreuung: Alexander Weigl (ITI Beckert) weigl@kit.edu

Deck- und kartenminimale spielkartenbasierte sichere Mehrparteienberechnung

Kryptographie ist weit mehr als nur Verschlüsselung. Mit der sogenannten sicheren Mehrparteienberechnung können verschiedene Akteure gemeinsam eine Funktion berechnen, ohne dabei etwas über die privaten Eingaben der jeweils anderen zu lernen (das nicht bereits durch die Ausgabe offensichtlich ist). So können z. B. Zwei Spieler durch Berechnung eines logischen UNDs bestimmen, ob gegenseitiges romantisches Interesse besteht, ohne dass bei nur einseitigem Interesse die Gefahr besteht, dass die jeweils andere Person dies erfährt. Im Bereich der „Spielkartenbasierten Kryptographie“ braucht man hierfür nur ein paar Spielkarten mit ununterscheidbarer Rückseite – es geht also gänzlich ohne Computer. Neben dem Schutz vor Trojanern, die einfach die Eingabe mitlesen, sind diese kryptographischen Protokolle vor allem für die Demonstration von sicherer Mehrparteienberechnung in didaktischen Kontexten interessant. Ein Ziel ist es, solche Protokolle zu entwerfen, die möglichst wenig Karten verwenden und z. B. durch die geeignete/eingeschränkte Wahl der Mischoperationen auf den Karten einfach durchführbar sind.
Der Großteil der Literatur verwendet Decks die auf den Vorderseiten nur die Symbole Herz (♥) und Kreuz (♣) haben. Wir möchten stattdessen Protokolle entwerfen, die z. B. ein einziges Standard-Spielkarten-Deck mit sämtlich unterscheidbaren Symbolen 1, …, 52 verwenden, oder untere Schranken für die Anzahl von Karten in UND-Protokollen in diesem Setting beweisen. Je nach Einschränkung an die Mischoperation sind hierfür auch Vorkenntnisse im Bereich der Gruppentheorie (Gruppenaktionen, Orbit, Stabilisator, etc.) hilfreich.

Kontakt/Betreuung: Alexander Koch (ITI Müller-Quade) alexander.koch@kit.edu

Kontinuierliche Haptische Interfaces in Videospielen

Haptische und taktile Interfaces sind besonders Bereich der Konsolenspiele ein wichtiger Bestandteil der Spiele um Informationen an den Spieler zu übertragen und Immersion zu schaffen. In „klassischen“ Videospielen mit Maus und Tastatur sind haptische und taktile Interfaces allerdings kaum anzutreffen. Mit Smartwatches, Fitnesstrackern und anderen Wearables gibt es nun die Möglichkeit, haptische und taktile Interfaces für Videospiele mit Maus und Tastatur zu schaffen.
Ziel des „Praxis der Forschung“-Projekts ist es daher, auf Basis des am TECO entwickelten Wearables verschiedene Strategien zur kontinuierlichen taktilen Informationsvermittlung zu entwickeln und in Laborstudien auf deren Effektivität und Nutzerfreundlichkeit zu testen. Themengebiete sind dabei die Anwendbarkeit von passivem Lernen (Passive Haptic Learning) und die parallele taktile Übertragung unterschiedlicher Informationen.

Kontakt / Betreuung: Erik Pescara (TM Beigl) pescara@teco.edu

Quellcodeverständnis und API Usability

Das Entwickeln von Software erfordert das Verstehen von Quellcode, ob beim Entwickeln neuer Software, bei der Wartung bestehender Software oder beim Integrieren neuer Funktionalitäten. Dabei kann das Lesen und Verstehen bereits vorhandenen Codes sowie des Stils und der Intention des ursprünglichen Entwicklers länger dauern als das eigentliche Integrieren der Funktion. Zu erforschen, wie Entwickler Quellcode verstehen, kann zu verbessertem Quellcode führen, der es zukünftigen Entwicklern erleichtert, vorhandene Software zu pflegen und zu erweitern. Das ist insbesondere für die Entwicklung von APIs von Bedeutung. Obwohl es Empfehlungen und Konventionen zum Schreiben von Quellcode gibt (z.B. Java-Konventionen oder Clean Code), liegen bislang nur wenige empirische Befunde vor, die diese Empfehlungen prüfen.
Ziel des „Praxis-der-Forschung-Projekt“ ist daher die empirische Untersuchung, wie Programmierer Quellcode verstehen. Dazu sollen empirische Studien geplant, durchgeführt und ausgewertet werden. Je nach Interesse kann entweder eher auf die Erforschung von kognitiven Prozessen (Aufmerksamkeit oder Gedächtnis) oder auf die Usability von APIs fokussiert werden.

Kontakt / Betreuung: Dr. Andrea Schankin (TM Beigl) andrea.schankin@kit.edu

Machine Learning in Communication Networks

Machine learning – especially deep reeinforcement learning – is currently one of the most emerging research areas in computer science, beeing at the top peak of the Gartner Hype Cycle in 2017. In the last year, Libratus from Carnegie Mellon university beat four of the world’s best professional poker players. AlphaGo Zero from Google DeepMind beat the world’s best chess-playing computer programs after teaching itself how to play in only four hours. And there are countless other examples from a broad range of different domains that underline the importance of machine learning, from personal assistents via self-driving cars to smart health care.
It is thus not surprising that machine learning is applied to communication networks as well. Because the complexity of communication networks has grown tremendously in the past 10 years, new scalable and efficient techniques are required for network management, measurement, security or analysis. And machine learning is one promising candidate to achieve this.
In this project, we first want to understand and classify existing approaches where machine learning is applied to different aspects of communication networks. Based on this preparatory work, we will develop a novel concept where machine learning is applied to one of the existing projects at our Institute. For implementation, it is planned to rely on open-source machine learning frameworks such as TensorFlow or PyTorch. We currently have several ongoing projects that qualify for a machine learning approach: (1) Congestion Control, (2) Flow Delegation, (3) DDoS Mitigation, (4) Network Resilience, and (5) Predictive Maintenance.

Kontakt / Betreuung: Robert Bauer (TM Zitterbart) robert.bauer@kit.edu
Hauke Heseding (TM Zitterbart) hauke.heseding@kit.edu