Profil: Software Engineering Research am AIT - Austrian Institute of Technology GmbH

Rupert Schlick[1]

Abstract: Dieser Artikel stellt das Forschungsinstitut AIT Austrian Institute of Technology GmbH vor und beleuchtet seine Rolle als Transfer-Institut für Forschung zum Software Engineering. Dazu werden einerseits die zum Thema passenden, bestehenden Aktivitätsschwerpunkte kurz vorgestellt, andererseits aktuelle Verwertungspfade berichtet und bewertet.

Keywords: Profil Transfer-Institut; Österreich; Infrastrukturbezogene Forschung

1 AIT - ein Transfer-Institut

1.1 AIT - Austrian Institute of Technology GmbH

Das *AIT Austrian Institute of Technology* ist Österreichs größte außeruniversitäre Forschungseinrichtung. Mit seinen acht Centern versteht sich das AIT als hochspezialisierter Forschungs- und Entwicklungspartner für die Industrie. Durch die Forschung und technologischen Entwicklungen des AIT werden grundlegende Innovationen für die nächste Generation von Infrastrukturtechnologien in den Bereichen *Energy, Mobility Systems, Low-Emission Transport, Health & Bioresources, Digital Safety & Security, Vision, Automation & Control* und *Technology Experience* verwirklicht. Ergänzt werden diese wissenschaftlichen Forschungsgebiete um die Kompetenz im Bereich *Innovation Systems & Policy*.

Rund 1.300 MitarbeiterInnen forschen in ganz Österreich - im Besonderen an den Hauptstandorten Wien Giefinggasse, Seibersdorf, Wr. Neustadt, Tulln, Ranshofen und Graz – an der Entwicklung jener Tools, Technologien und Lösungen für Österreichs Wirtschaft, die sie gemäß unseres Grundsatzes „Tomorrow Today“ zukunftsfit halten.

Gesellschafter des AIT sind die Republik Österreich (Bundesministerium für Verkehr, Innovation und Technologie), die 50,46% der Anteile hält und der Verein zur Förderung von Forschung und Innovation (Industriellenvereinigung Österreich) mit 49,54% der Anteile.

[1] AIT Austrian Institute of Technology GmbH, Center for Digital Safety and Security, Giefinggasse 4, 1210 Wien, Österreich, rupert.schlick@ait.ac.at

doi:10.18420/SE2020_59

1.2 Center for Digital Safety & Security

Im *Center for Digital Safety & Security* werden modernste Informations- und Kommunikationstechnologien (IKT) und Systeme entwickelt, um kritische Infrastrukturen im Kontext der umfassenden und globalen Vernetzung und Digitalisierung sicher und zuverlässig zu gestalten.

Dabei fokussiert das Center auf folgende Schlüsseltechnologiebereiche: Cyber-Sicherheit für Industrial Control Systems (ICS), Cyber Physical Systems (CPS), und Internet of Things (IoT), hochsichere und hochverfügbare Software und Systeme sowie höchst zuverlässige Wireless-Kommunikation der nächsten Generation (5G), modernste Verschlüsselungsmethoden (Quantum Safe) für virtuelle IT-Systeme, Data Science für neue Ansätze eines modernen Datenmanagements (Big Data, Blockchain-Technologien), als auch neueste Sensortechnologien und Systeme zum Schutz kritischer Infrastrukturen, Command und Control Systeme für den Einsatz im modernen Krisen- und Katastrophenmanagement sowie Objektschutz kritischer Infrastrukturen und digitales Identity Management durch modernste Biometrie-Sensorik.

In enger Kooperation mit Wirtschaft und Industrie, Wissenschaft und öffentlicher Hand erfolgt eine strategische Technologieforschung sowie Entwicklung von Prototypen bis hin zur Validierung von Anwendungen in disruptiven Öko-Systemen. Das Center for Digital Safety & Security besitzt in nationalen und internationalen Innovationsprogrammen der Sicherheitsforschungsprogramme eine anerkannte Position und baut auf strategischen Partnerschaften mit den wichtigsten nationalen Sicherheitsakteuren (BMI und BMLVS) als auch in internationalen Industrieinitiativen wie beispielsweise ECSO (European Cyber Security Organisation) [2], PSCE (Public Safety Communication Europe) [3], EARTO/EUROTECH Sicherheitsgruppe (Task Force europäischer Forschungsorganisationen im Sicherheitskontext) [4], ARTEMIS/ECSEL (Europäische Technologie- und Forschungsplattform im Bereich eingebetteter und cyberphysikalischer Systeme) [5], EPoSS (Europäische Technologie- und Forschungsplattform im Bereich der Integration intelligenter Systeme) [6] und euRobotics [7] auf.

2 Themenkreise Software Engineering

Forschung im Umfeld Software Engineering findet primär in der *Competence Unit for Secure Communication Technologies* im Forschungsfeld *Dependable Systems Engineering* statt. Die hier bearbeiteten Themen fallen durchwegs in Rand- und Nischenbereiche des

[2] https://www.ecs-org.eu/
[3] http://www.psc-europe.eu/
[4] http://www.earto.eu/
[5] https://www.artemis-ju.eu/
[6] https://www.smart-systems-integration.org/public
[7] https://www.eu-robotics.net/

klassischen Software Engineering und zielen, passend zur Ausrichtung des Unternehmens, auf die Absicherung der Zuverlässigkeit und Betriebssicherheit geschäfts- und infrastrukturkritischer, softwarelastiger Systeme.

Die Arbeiten gliedern sich grob in die Themenkreise *Safety & Security Co-Engineering*, *Model-Based Testing* und *Runtime Verification und Monitoring*. Die zum Einsatz kommenden Methoden bedienen sich im Software-Prozess-Entwurf ebenso wie bei Theorien zum Software-Test, im Maschinellen Lernen und bei der Formalen Verifikation und Formalen Methoden.

2.1 Safety & Security Co-Engineering für Cyber-Physical Systems

Obwohl für Steuerungssysteme generell und für sogenannte Cyber-Physical Systems im besonderen, sowohl Aspekte der Betriebssicherheit (*Safety*, Schutz von Werten, Gesundheit, Leben und Umwelt vor Auswirkungen eines Systemversagens) als auch der Manipulationssicherheit(*Security*, Schutz des Systems, seiner Betriebsfähigkeit und der damit verbundenen Werte vor unberechtigtem Zugriff, Manipulation und Sabotage)[8] besonders wichtig sind und einige Gemeinsamkeiten aufweisen, sind die zugehörigen Forschungs-Communities nach wie vor sehr klar getrennt. Sowohl für Safety als auch für Security spielt die Berücksichtigung im System-Entwurf (Safety and Security by Design) und ihre Sicherstellung in Implementierung und Betrieb eine wichtige Rolle. Die mögliche gegenseitige Beeinflussung (z.B. im Entwurf hinzugefügte Safety-Mechanismen verändern die Angriffs-Oberfläche für Security-Betrachtungen; ein Security-Incident deaktiviert Safety-Mechanismen) legt nahe, die beiden Aspekte im Entwicklungsprozess auch ganzheitlich zu berücksichtigen. AIT ist hier in folgenden Bereichen aktiv:

Safety- und Security-Standardisierung Die Bereiche safety-kritischer Systeme, wie Eisenbahnwesen, Flugverkehr, chemische Anlagen, medizinische Systeme und Automobile, sind hochgradig reguliert, Standards spielen in dieser Regulierung eine wesentliche Rolle. AIT Mitarbeiter sind aktive Mitglieder einer Reihe einschlägiger Standardisierungsgremien in diesem Bereich. Dazu zählen z.B. ISO 26262, ISO/PAS 21448, ISO/SAE 21434, ISO 13849, IEC TR 63074, IEC 61508, IEC TR 63069 und IEC 62443-(1-4). Anzumerken ist hier, dass AIT (und seine Vorgänger-Organisationen) seit mittlerweile Jahrzehnten auf die Berücksichtigung von Security in den Safety-Standards hinwirkt.

Safety & Security Co-Analyse Um Safety & Security by Design sicher zu stellen, arbeitet AIT an Methoden und Werkzeugen sowohl zur Identifikation und Addressierung von

[8] im Folgenden wird, im Interesse einer klareren Begrifflichkeit, mit den englischen Begriffen Safety und Security gearbeitet

Bedrohungen für CPS (Tool *ThreatGet*[9]) als auch zur Identifikation und Fortpflanzung von Safety- und Security-Problemen in CPS [Sc14; SMS14].

Safety-Case Management Verschiedene Safety Standards stellen verschiedene Anforderungen an die Entwicklungs- und Qualitätssicherungs-Prozesse. Das Tool GSFlow [10] unterstützt die Verwaltung von Argumentation und Evidenz für *Safety Cases* passend zu und konfigurierbar für eine Reihe einschlägiger Standards.

2.2 Model-Based Testing

Forschungsthema ist auch die automatisierte Erstellung von Tests, typischerweise aus Modellen. Die Generierung funktionaler Tests wird hier derzeit erweitert um Tests zum Erfüllungsnachweis nicht-funktionaler Anforderungen wie Safety, Performance oder Robustheit. Ergebnis aus und Plattform für diese Forschungsaktivitäten ist die Familie von Testfallgeneratoren *MoMuT*[11]. Aktuelle Arbeiten zielen auf die Unterstützung im Modellierungsprozess und den Review von (formalen und semi-formalen) Verhaltensmodellen durch den Review daraus generierter Tests [SK19; Sn18] sowie die Integration in Modellierungsumgebungen wie *Enterprise Architect* von *SparxSystems*.

2.3 Runtime Verification

Hier werden formale Definitionen von Systemverhalten, zum Beispiel Signalverläufe, verwendet, um im Betrieb automatisch Abweichungen (z.B. zu flache Flanke, Ereignis komt zu früh / zu spät / zu oft) zu erkennen. „Im Betrieb“ bedeutet hier nicht unbedingt im Produktiveinsatz, sondern auch etwa im Bereich des End-Tests von Hardware-Komponenten. Aktuell wird an Möglichkeiten geforscht, die formalen Definitionen automatisch von einem korrekt funktionierenden System abzuleiten oder die Parameter eines Templates anzulernen. [Ni19]

3 Transferpfade

3.1 Ko-finanzierte Forschung

Der Löwenanteil der Arbeiten der Gruppe erfolgt im Rahmen nationaler und europäischer kofinanzierter Forschungsprojekte, vorwiegend in Forschungslinien, die Forschungs-Transfer

[9] https://www.threatget.com/
[10] http://gsflow.ait.ac.at/
[11] http://momut.org

adressieren, wie *IKT der Zukunft*[12] der *FFG* in Österreich und IA- und RIA-Projekte in Projekten des *ECSEL Joint Undertaking*[13] mit gemischt nationaler und EU-Förderung, aber auch *H2020 ICT*[14] und EUROSTARS[15]. Kürzlich abgeschlossene oder aktuell laufende Projekte sind zum Beispiel AQUAS, AutoDrive, Comp4Drones, IoT4CPS, TRUCONF, EMBEET, ENABLE-S3 und SEMI4.0.

3.2 Beratung und Training, Forschungsaufenthalte

Einen deutlich geringeren Teil der Aktivitäten machen Industrieaufträge für Beratung oder die Erstellung von Studien aus. Erwähnenswert ist hier eine Kooperation mit Toyota USA zu spezifikationsbasierten Verifikationsmethoden zu Entwicklungs- und Lauf-Zeit. Forschungsthemen sind hier: Spezifikationssprachen für CPS-Anwendungen (Automobil und Robotik), Sensitivitätsanalysen in Verbindung mit formalen Spezifikationen, Suchbasierte Tests, automatisierte Kausalitätsanalysen bei Ausfällen.

3.3 Lizenzierung

Die im Rahmen der Forschungsarbeiten entstandenen Werkzeuge werden teilweise selbständig oder in Kooperation mit Partnern so weit verbessert, dass sie für den industriellen Einsatz tauglich sind. Die Lizenzierung an Endkunden erfolgt dann vorzugsweise über einen Verwertungspartner. Der Transferpfad wird in der Gruppe erst jetzt, vorwiegend im Rahmen noch junger Kooperationen, genützt.

4 Beobachtungen und Konklusio

Die Erfahrung zeigt, dass man mit der Bearbeitung eines Themas selten warten kann, bis der Markt nach der Lösung für ein Problem fragt (Pull). Aber das Entwickeln von Lösungen für antizipierte Probleme (Push) bringt mit sich, dass man nicht nur inhaltlich, sondern auch zeitlich gründlich daneben liegen kann. So hebt derzeit das in der Gruppe eher junge Thema Safety- und Security Co-Analyse, speziell das Thema modellunterstützte Gefährdungsanalyse, zügig ab, während sich beim schon recht lange betriebenen Model-Based-Testing schleppend erste Lizenzerträge einstellen.

AIT ist ein etablierter und willkommener Partner in wissenschaftlichen Förderprojekten, auch im Umfeld von SE-Themen. Das hat allerdings zur Folge, dass längerfristig zu entwickelnde

[12] https://www.ffg.at/iktderzukunft
[13] https://www.ecsel.eu/
[14] https://ec.europa.eu/programmes/horizon2020/en/h2020-section/information-and-communication-technologies
[15] https://ec.europa.eu/programmes/horizon2020/en/h2020-section/information-and-communication-technologies

Themen von der österreichischen Industrie kaum beauftragt, sondern bevorzugt gemeinsam in geförderten Projekten erarbeitet werden. Die bunte Mischung an Themen, Fertigkeiten und genutzten Verwertungspfaden in der Gruppe bindet zwar Kräfte und erschwert das Erreichen kritischer Massen, bietet aber auch Sicherheit durch mehrere Standbeine in einem inhaltlich sehr bewegten Umfeld.

Literatur

[Ni19] Ničković, D.; Qin, X.; Ferrère, T.; Mateis, C.; Deshmukh, J.: Shape Expressions for Specifying and Extracting Signal Features. In (Finkbeiner, B.; Mariani, L., Hrsg.): Runtime Verification. Springer International Publishing, Cham, S. 292–309, 2019, ISBN: 978-3-030-32079-9.

[Sc14] Schmittner, C.; Gruber, T.; Puschner, P.; Schoitsch, E.: Security Application of Failure Mode and Effect Analysis (FMEA). In (Bondavalli, A.; Di Giandomenico, F., Hrsg.): Computer Safety, Reliability, and Security. Springer International Publishing, Cham, S. 310–325, 2014, ISBN: 978-3-319-10506-2.

[SK19] Schlick, R.; Krenn, W.: Tackling the Challenges of Internet-of-Things-Development Using Models. In. DATE 19, 2nd International ESIIT Workshop. Florence, Italy, S. 40–41, März 2019, URL: http://adt.cs.upb.de/ESIIT2019-tproceedings.pdf.

[SMS14] Schmittner, C.; Ma, Z.; Smith, P.: FMVEA for Safety and Security Analysis of Intelligent and Cooperative Vehicles. In (Bondavalli, A.; Ceccarelli, A.; Ortmeier, F., Hrsg.): Computer Safety, Reliability, and Security. Springer International Publishing, Cham, S. 282–288, 2014, ISBN: 978-3-319-10557-4.

[Sn18] Snook, C. F.; Hoang, T. S.; Dghaym, D.; Butler, M. J.; Fischer, T.; Schlick, R.; Wang, K.: Behaviour-Driven Formal Model Development. In: Formal Methods and Software Engineering - 20th International Conference on Formal Engineering Methods, ICFEM 2018, Gold Coast, QLD, Australia, November 12-16, 2018, Proceedings. S. 21–36, 2018, URL: https://doi.org/10.1007/978-3-030-02450-5%5C_2.