Software Certification: Methods and Tools

Dagstuhl-Seminar 13051 Preliminary Program

Status

25.1.13 11:00 PM

	Monday, 27.01.	Tuesday, 28.01.	Wednesday, 29.01.	Thursday, 30.01.	Friday, 31.01.
	Welcome Session	Assurance Cases and Evidence	Medical Domain Challenges	Model-Based Development of Critical Systems	Discussion
09:00	*Organizers Goals, Dagstuhl Protocols*	*Tim Kelly , University of York*	*John C. Knight , University of Virginia*	*Dominique Blouin, Université de Bretagne Sud*	*Next Steps*
		Software Certification: Where is Confidence Won and Lost?	Complex Medical System Dependability - The Same or Different?	Modeling Requirements of Embedded Systems with RDAL	*Planning for Seminar Outcomes*
		Janusz Gorski , Gdansk University of Technology	*Andrew King , University of Pennsylvania*	*Brian Larson, Multitude Corp.*	
	Intro per participant: 2 min	Bringing evidence-based arguments into practice	Certification Challenges in Medical Systems of Systems	Artifacts for Mock Certification Submission	
		John Rushby, SRI	*Jens H. Weber , University of Victoria*	Jerôme Hugues, ISAE - Toulouse	
		Logic and Epistemology in Assurance Cases	Certification of Medical Information Systems - A paradigm shift: from devices to systems, from functions to data	Bridging the modeling/verification gap	
10:30	**Coffee**	**Coffee**	**Coffee**	**Coffee**	**Coffee**
	Domain Overviews	Tool Support in Certification		Model-Based Development of Critical System	Discussion
11:00	*Virginie Wiels*	*Cyrille Comar, AdaCore, Paris*	*Jozef Hooman, Radboud University Nijmegen*	*John S. Fitzgerald, Newcastle University*	*Next Steps*
		Integrating Formal Program Verification with Testing	Software verification in the medical domain	Formal Models, Formal Methods and Assurance	*Planning for Seminar Outcomes*
	Avionics Overview	Jan Philipps, Validas AG - München	*Michael Holloway, NASA Langley ASDC - Hampton*	*Dominique Mery, LORIA - Nancy*	
		From Tool Qualification to Tool Chain Design	Concerning the implicit DO-178C assurance case	Refinement may help for Certification	
11:30	*Alan Wassyng*	*Daniel Kaestner , AbsInt - Saarbrücken*	*Bernhard Schätz, fortiss GmbH, München*	*András Pataricza*	
	Nuclear Domain Overview	Using Code Analysis Tools for Software Safety Certification	Model-Based Approaches to Software Certification	Models and certification	
12:15	**Lunch**	**Lunch**	**Lunch**	**Lunch**	**Lunch**
	Domain Overviews	Assurance and Confidence	**Excursion to Trier starting 13:30**	Model-Based Development of Critical Systems -continued	
14:00	*John Hatcliff, John Knight, Mats Heimdahl, Je*	*John McDermid, University of York*	Departure: 13:30 !	*Hubert Garavel , INRIA Rhône-Alpes*	**- End of the Seminar -**
	Medical Domain Overview	Software Certification: The Return on Investment?	We will join with the other group on Cyberphysical Multicore Systems and have a guided tour in Trier	A naive look at software certification practices - and some enhancement proposals	
		Kim Fowler, Kansas State University	Chane of plans: After some free time we will return to Dagstuhl and have dinner at Dagstuhl (the Winery announced some difficulties, sorry)	*Julia Rubin , IBM - Haifa*	
		What is Mission-Assurance? (and how do we achieve it?)		Cloud Security: Information Segregation and Data Privacy	
	Mirko Conrad, Mathworks	*Tom S. Maibaum, McMaster University - Hamilton*		*David von Oheimb, Siemens AG - München*	
		Bayesian Probabilistic Approaches to		Activities around security certifications	
	Software 'Certification' in the Automotive Domain	Confidence are Impossible: the need for a Baconian Approach		according to the Common Criteria at Siemens Corporate Technology	
15:30	**Coffee & Cake**	**Coffee & Cake**	**Excursion to Trier starting 13:30**	**Coffee & Cake**	**Coffee & Cake**
	Domain Overview & Discussion	*Hardi Hungar, German Aerospace Center - Braunschweig*		Static Analysis	
16:00	Domain Assessment	Rail Domain and Open Source		*Arie Gurfinkel, CMU - Pittsburgh*	
	Differences between domains	*Peter Karpati (Inst for Energy Technology, Halden, Norway)*		Static Analysis of Real-Time Embedded Systems with REK	
	Similarities between domains	Towards an Effective Safety Demonstration Framework		*Richard F. Paige, University of York*	
	Challenges (break out groups, + reconvene + vote)	Challenge Problem Advertisements		Certification of a (Run-Time) Safety Language and System	
	General challenges,	*Pacemaker, PCA, Avionics (Rockwell Collins / NASA), Nose Gear*		*Dominik Mader, Berner & Mattner*	
	Domain challenges	Discussion	**Returnto Dagstuhl: About 18:00**	Automotive Software Certification and Testing	
	Seminar Outcomes: *Collection of papers Challenge problems, Example artifacts*				
18:00	**Dinner**	**Dinner**	**Dinner**	**Dinner**	**Dinner**