In conjunction with the
SAFECOMP 2016 Conference
http://www.safecomp.org

SafeComp 2016
international conference on computer safety, reliability and security
20-23 September | Trondheim | Norway

ASSUME Waruna

1st TIPS'16 Workshop

*1st International workshop on the **TI**ming **P**erformance in **S**afety Engineering*

20 September 2016,
Trondheim, Norway

AGENDA

09:00	**TIPS'16 WELCOME & Agenda –**	**L. Rioux, M.C.W Geilen**
09:15	ASIL-conformant deployment and schedule synthesis using multi-objective design space exploration	Sebastian Voss (FORTISS/TUM)
10:15	Model-based Component Contracts and Online Services for Self-managed Integration of General Purpose Components in Safety & Time-Critical Cyber-Physical Systems	DeJiu Chen (KTH, Sweden)
11:00	**BREAK**	
11:30	Model-Based real-time evaluation of security patterns: A SCADA system case study	Anas Motii, Agnes Lanusse, Brahim Hamid and Jean-Michel Bruel
12:00	Automotive Ethernet: Towards TSN and Beyond	Zhonghai Lu (KTH, Sweden)
12:30	An industrial timing verification challenge and some solutions	P. Reinkemeier (OFFIS)
13:00	**LUNCH**	
14:00	Dataflow-based verification of temporal properties for virtualized multiprocessor systems	M. Skelin (TU Eindhoven)
14:30	WARUNA Project: Modeling and Timing Verification Framework	R. Henia (THALES)
15:00	ASSUME Project: Objectives and current	L. Rioux(THALES)

	status	
15:30	**BREAK**	
16:00	PANEL “new Challenges for Timing Performance for Safe CPS”	C. Mraidha, L. Rioux, S. Voss, M.C.W Geilen
16:45	Conclusions & Closing Remarks	L. Rioux, M.C.W Geilen
17:00	End of the workshop	

Contacts:

Laurent Rioux, laurent.rioux@thalesgroup.com; M.C.W Geilen, M.C.W.Geilen@tue.nl

ABSTRACTS of INVITED TALKS

Title: **Model-based Component Contracts and Online Services for Self-managed Integration of General Purpose Components in Safety&Time-Critical Cyber-Physical Systems**

DeJiu Chen <chen@md.kth.se> Mechatronics, Machine Design, KTH Royal Institute of Technology, Sweden

Abstract: Modern automotive vehicles represent one category of cyber-physical systems that are inherently safety & time-critical. Future automotive technology will to an increasingly large extent be based on general purpose electronics for shortening the innovation loops and enabling efficient product evolution. Nevertheless, the adoption of general purpose electronics in automotive vehicles will not be a trivial task. Currently, while domain-specific frameworks like AUTOSAR facilitate the use of “off-the-shelf” components, challenges remain in the areas of contract synthesis, conformity assessment, and diagnostics when issues like mode behaviors, timing, and failures are of concern. Safety standards like ISO-26262 allow the development of components for safety critical systems based on well-formulated assumptions. There are however still challenges related to the formalization, elicitation and communication of safety requirements and how to effectively guarantee the compositionality and composability. This talk presents the EAST-ADL modeling framework and discusses an EAST-ADL based approach to system modularity and risk analysis in order to integrate separately developed electronic components into safety-critical automotive systems. Special attention is paid to the synthesis of both component contracts and the associated runtime services for lifecycle and quality management, anomaly treatment according to ISO-26262.

Title: **Automotive Ethernet: Towards TSN and Beyond**

Zhonghai Lu <zhonghai@kth.se>, Electronics and Embedded Systems, KTH Royal Institute of Technology, Sweden

Abstract: As a new generation of E/E architecture, Ethernet is rapidly penetrating into the automotive domain. To accommodate the timing requirements of automotive applications, Ethernet is evolving to support time-sensitive networking (TSN) with mixed criticality. This talk will first present a landscape brought by TSN for advanced driver assistance systems (ADAS). Then we will

exemplify how the TSN can better cope with application requirements than conventional Ethernet, in particular, in adaptively delivering QoS assurances under vehicle internal and external situations. Finally we shall discuss challenges and opportunities on deploying TSN for advanced automotive applications under safety concerns.

Title: **An industrial timing verification challenge and some solutions**
Philipp Reinkemeier <Philipp.Reinkemeier@offis.de>, OFFIS, Germany

Abstract : Timing and scheduling analysis is an important step in safety relevant embedded system design for many application domains, such as avionics, automotive and automation. Increasing system complexity, not least due to multi-core architectures and a shift to integrated architectures concentrating large number of functions on control units, requires constant evolution of the analysis approaches.
In this talk the timing and scheduling analysis challenges of an avionics case study from the ASSUME project are presented, as well as an approach to verify complex timing requirements part of this case study.

Title: **Dataflow-based verification of temporal properties for virtualized multiprocessor systems**
Mladen Skelin and Marc Geilen <m.skelin,m.c.w.geilen@tue.nl> , Eindhoven University of Technology, Eindhoven, The Netherlands

Abstract: Over the last decade we have witnessed ever increasing use of virtualized multiprocessor platforms in the design of advanced digital systems. This is due to the fact that virtual platforms, by means of virtual machines, facilitate the design of complex systems involving large numbers of applications by providing both spatial and temporal isolation between them. In particular, each application is assigned with a fraction of the platform's (spatial and temporal) capacity and can be treated as if it were executing on a platform of its one. This means that in cases where applications have stringent temporal constraints we can analyse their temporal behavior in isolation because the behavior of one is not a reflected by the other. In this talk we reflect on the model-based design flow developed at Eindhoven University of Technology that by the use of aforementioned virtualization principles guarantees composability and predictability. In particular, we discuss how timed data flow-based design flow implemented in the SDF3 tool enables real-time data flow applications to be automatically mapped, verified and executed on the CompSOC temporally composable platform providing strongly temporally isolated virtual multiprocessor platforms.

Title: **WARUNA project: Modeling and Timing Verification Framework**
Rafik Henia <rafik.henia@thalesgroup.com>, THALES R&T, France

Abstract: WARUNA is a French research project aiming at developing a framework to model and verify timing properties in real-time embedded systems. The framework covers all design phases and allows evaluating the impact of the design decisions on the response times. It also allows merging the timing results obtained at different design levels from the different analysis tools. The WARUNA framework is integrated in the modeling environment. In the talk, the WARUNA framework will be presented, as well as the project objectives and the partners' role. More details about the WARUNA project can be found on the project website: http://www.waruna-projet.fr/.