Abstract for Poster contribution at MESS'16, Vienna:

Egbert Althammer, Erwin Schoitsch, AIT Austrian Institute of Technology
{Egbert.althammer, erwin.schoitsch}@ait.ac.at

WEFACT: A Prototype Implementation of an Interoperability Specification (IOS)

Interoperability is a two-fold issue: Interoperability of system components/interfaces, or interoperability of tools. This is most important for safety critical cyber-physical systems. Functional safety standards like IEC 61508 (generic), ISO 26262 (automotive) or EN 50128/29 (rail) have qualification criteria/requirements for tools to be applied, but there is no provision how to tackle the tool-chain issue. Several ARTEMIS projects (CESAR, SafeCer, MBAT, CRYSTAL, EMC²) have developed stepwise an approach towards an IOS, each step based on results of previous projects. To harmonize these approaches, the ARTEMIS Standardization WG started the H2020 Innovation Action CP-SETIS, including major partners from the related projects, to create a sustainable structure/eco-system to maintain and further develop IOS. It was identified that IOS has to be a collection of standards and specifications (and not a single one) for seamless integration of tools-, methods- and processes. An IOS Coordination Forum (ICF) hosted by an established organization to maintain IOS and spread the information to the community will be created. First IOS implementations are based on OSLC (Open Services for Lifecycle Collaboration, OASIS Consortium). An example is the Workflow Tool WEFACT (Workflow Engine for Analysis, Certification and Test) covering the whole V&V cycle from requirements to certification/qualification.

Acknowledgements: Parts of this work were funded by the European Commission under grant agreement 645149 (Horizon 2020 Innovation Action CP-SETIS), grant agreement 269335 (ARTEMIS project MBAT) and grant agreement 295373 (ARTEMIS project nSafeCer).

Assertion-based Verification Framework for Cyber-Physical Systems

Dejan Nickovic
AIT Austrian Institute of Technology GmbH.

Functional system correctness and safety standard compliance can be guaranteed only by using methodologies and tools that cover the full chain from requirement definition via design/implementation up to the validation phase. We propose an assertion-based verification and validation (V&V) framework that can serve as an interface among all parties in the value chain, by enabling a uniform exchange of system and sub-system requirements of cyber-physical systems.

The central idea is to use assertions as a uniform language to specify formal and unambiguous requirements and exchange them between actors in the value chain. The assertion languages enable reuse across multiple orthogonal axes:

1. Across different phases of the design work-flow (design simulation, its FPGA emulation and lab evaluation);
2. Along various actors in the supply chain (Tier 2, Tier 1 and OEM);
3. Across verification tools, including monitoring, model-based testing and model checking.

The key to the successful adoption of such a framework in industry is the standardization of the assertion language and the interoperability of tools supporting the methodology. This objective can be met by combining tool support for standard assertions and connecting the tools by using the Interoperability Specification (IOS) based on OSLC (Open Services for Lifecycle Collaboration). These aspects are the focus of our current and future research and should be a contribution to the CP-SETIS Interoperability Framework.

Acknowledgement: Part of this work is funded by the European Commission under grant agreement 645149 (Horizon 2020 Innovation Action CP-SETIS)