

System-Software Co-Engineering: Dependability and Safety Perspective

Y. Yushtein,
Systems, Software & Technology Department,
European Space Agency,
Noordwijk, NL,
yuri.yushtein@esa.int

J.-P. Katoen, V.Y. Nguyen, Th. Noll,
Software Modeling and Verification Group,
RWTH Aachen University, D,
{katoen,nguyen,noll}@cs.rwth-aachen.de

M. Bozzano, A. Cimatti, M. Roveri,
Embedded Systems Research Unit,
Fondazione Bruno Kessler, Trento, I,
{bozzano,cimatti,roveri}@fbk.eu

X. Olive,
Research Department,
Thales Alenia Space France,
Cannes la Bocca, F,
xavier.olive@thalesaleniaspace.com

Abstract—The need for an integrated system-software co-engineering framework to support the design of modern space systems is pressing. The current tools and formalisms tend to be tailored to specific analysis techniques and are not amenable for the full spectrum of required system aspects such as safety,

Keywords-correctness, dependability, fault tree analysis, model checking, performability, safety

such, the current practices lack integration and coherence. We recently developed a coherent and multidisciplinary approach towards developing space systems at architectural design level, linking all of the aforementioned aspects, and assessed it with several industrial evaluations. This paper reports on the approach, the evaluations and our perspective on current and future developments.

such, the current practices lack integration and coherence. We recently developed a coherent and multidisciplinary approach towards developing space systems at architectural design level, linking all of the aforementioned aspects, and assessed it with dependability and performability. Additionally, they cannot handle the intertwining of hardware and software interaction. As dependability and performability. Additionally, they cannot handle the intertwining of hardware and software interaction. As