Actionable definition of Safety Design Patterns using AADL, ALISA and the Error Modeling Annex

Submitted by hugues on Fri, 08/14/2020 - 11:42am. Contributor: Jerome Hugues

The AADL group at CMU/SEI is currently conducting a study to model these design patterns using the AADL and later relate them to actual system's architecture, but also to a verification plan. AADL provides a modeling framework for describing the architecture of hardware and platform resources, software components, and flexible allocation software components to resources. Through its annex languages and tool plug-in extensibility mechanisms, it also provides a variety of architecture analyses including hazard analysis, schedulability analysis, dependability analysis. In addition, ALISA supports the definition of assurance plan that relates an architectural description to a set of verification methods connected to formal analysis. In this talk, we will illustrate how to leverage AADL and its ecosystem to capture Safety design patterns as a library of model elements; capture for each pattern the corresponding abstract verification plan they presume; and then apply them to specific system instances. We will discuss different usage of AADL to ensure correct traceability between a design pattern definition and its instantiation, either through extension and refinement; or through the preservation of design patterns structural invariants based on a graph representation of the pattern. Hence, we illustrate how these models can be used as actionable definition of patterns.


Copyright 2020 Carnegie Mellon University. This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT. DM20-0728

Jerome Hugues is Senior Researcher at the Software Engineering Institute on the Assuring Cyber-Physical Systems team. He holds a PhD (2005) and an engineering degree (2002) from Telecom ParisTech. His research interests focus on design of software-based real-time and embedded systems and tools to support it. He is a member of the SAE AS-2C committee working on the AADL since 2005. Prior to joining the CMU/SEI, he was professor at the Department of Engineering of Complex Systems of the Institute for Space and Aeronautics Engineering (ISAE), in charge of teaching curriculum on systems engineering, safety-critical systems and real-time systems. He contributes to the OSATE, Ocarina and TASTE projects AADL toolchains.

Jerome Hugues

License: Creative Commons 2.5
Actionable definition of Safety Design Patterns using AADLv2, ALISA and the Error Modeling Annex

Presentation HCSS 2020