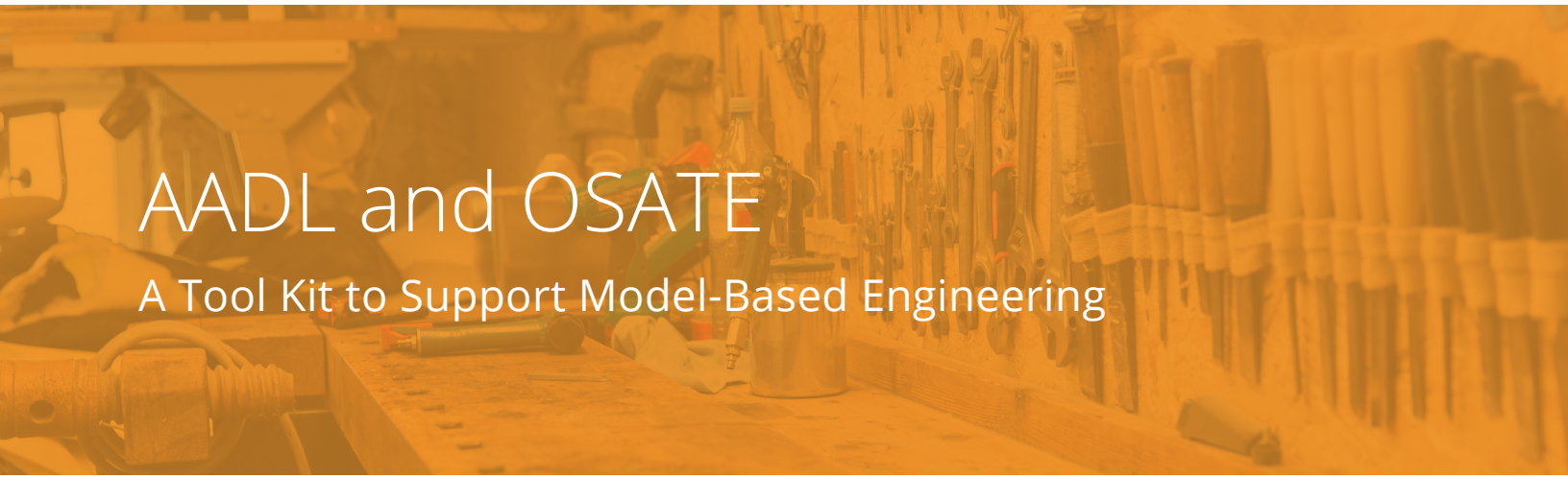
Carnegie Mellon University
Software Engineering Institute



AADL and OSATE

A Tool Kit to Support Model-Based Engineering

THE ARCHITECTURE ANALYSIS & DESIGN LANGUAGE (AADL) was developed by a committee of experts, with the SEI's Peter Feiler as technical lead, and sponsored by SAE International. It was approved as SAE Standard AS-5506 in 2004. Version 2.2 was published in 2017.

AADL supports software architects and developers in the predictable model-based engineering of real-time and embedded computer systems. Intended fields of application include automotive systems, avionics and space applications, medical devices, and industrial equipment.

The SAE AADL standard consists of a language with a precise semantics that allows users to define software and hardware components and their interactions. The standard defines two representations:

1. textual representation for language experts and model processing
2. graphical representation, convenient for communication purposes or editing a model in a user-friendly interface

The AADL committee extended the language to capture specific characteristics and define modeling patterns for specific architectures. The SEI led development of some of these extensions, including

- the Error Model Annex, a standardized AADL extension to support fault and reliability modeling as well as hazard analysis
- the ARINC 653 Annex, a set of model annotations and modeling patterns to capture ARINC 653 systems with their specific isolation requirements

AADL and example AADL models are available under the Eclipse Public License (EPL) in the SEI GitHub repository. Models are grouped into separate AADL projects that you can import into your workspace to test and experiment with.

The Open Source AADL Tool Environment (OSATE) Version 2

OSATE 2 is an Eclipse-based modeling framework for using AADL. In this environment, software architects can design and analyze models and then generate parts of the implementation code.

OSATE supports the textual and graphical representation of AADL. The textual editor features auto-indentation, auto-completion, and syntax highlighting. The graphical editor allows designers to revise the model, and it synchronizes the graphical and textual representations.

OSATE integrates several validation and analysis plug-ins. The SEI has developed tools for analyzing

- system safety
- system security
- performance
- flow latency
- scheduling
- resource budgeting (processor, weight, electrical power)

Each analysis produces reports in multiple formats—such as Excel and CSV—that facilitate discovery of potential issues and help designers build their architectures.

An Emphasis on Safety-Critical Systems

OSATE supports the Error Model Annex of AADL for specifying a system's fault behavior in the architecture model. Engineers can specify error occurrence and propagation in their architectures using the textual notation of AADL. OSATE includes several functions for processing this information and generating validation materials required by validation standards, such as

- Functional Hazard Assessment: description of faults that occur in each system function.
- Fault-Tree Analysis: occurrence of hierarchical dependencies between faults within the architecture. OSATE integrates its own Fault-Tree Analysis tool, EMFTA (see figure 1).

These tools have been evaluated and designed to support industrial practices, such as the SAE ARP4761 standard.

Toward Security Analysis

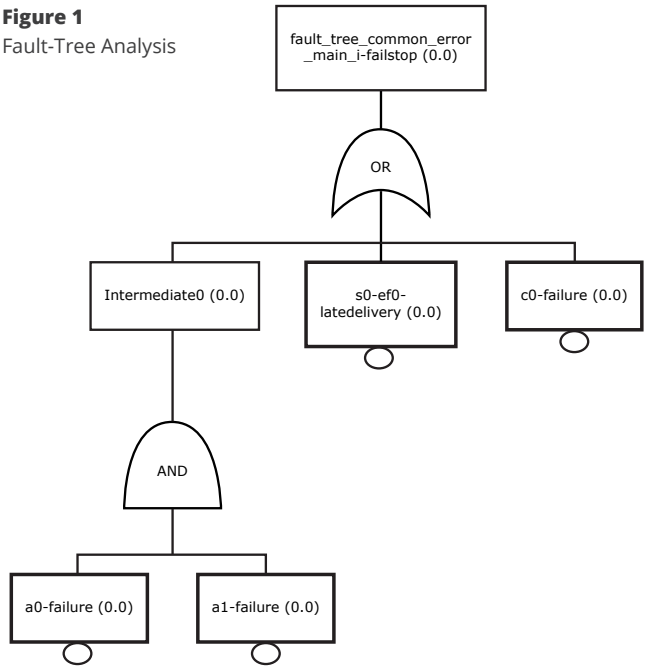
SEI researchers are developing security extensions for AADL. The next effort will produce a language annex to standardize specification of the security attributes of a system. The SEI team plans to design and release more security analysis tools, extending the number of analysis plug-ins available in the OSATE ecosystem. For example, a new Attack Impact Analysis function generates a graphical representation of how the vulnerabilities of each component may propagate through the system architecture. The SEI has released this tool as an experimental feature.

Additional Resources

AADL is available at **aadl.info**. Example models are available under the Eclipse Public License (EPL) in the SEI GitHub repository. Models are grouped into separate AADL projects that you can import into your workspace to test and experiment with.

OSATE is available at osate.org. The source code, plug-ins, and example models are available under the EPL in the SEI GitHub repository. Binary versions are available for Windows, Mac OS X, and Linux.

Figure 1
Fault-Tree Analysis



Wiki and Source Code

With our user community, the SEI maintains a wiki with all of our research on AADL that is accessible to the public: **wiki.sei.cmu.edu/aadl**

For more information about AADL and OSATE, visit the following web sites:

- AADL information page: **aadl.info**
- OSATE GitHub: **github.com/osate**
- OSATE download: **osate.org**

Publications, Webinars, Podcasts, and More

To learn more, visit SEI's collection of AADL resources at **resources.sei.cmu.edu/library/asset-view.cfm?assetid=453645**

Course Registration

Learn to model system architectures using AADL: **sei.cmu.edu/education-outreach/courses/course.cfm?courseCode=P72**

Training courses provided by the SEI are not academic courses for academic credit toward a degree. Any certificates provided are evidence of the completion of the courses and are not official academic credentials.

About the SEI

The Software Engineering Institute is a federally funded research and development center (FFRDC) that works with defense and government organizations, industry, and academia to advance the state of the art in software engineering and cybersecurity to benefit the public interest. Part of Carnegie Mellon University, the SEI is a national resource in pioneering emerging technologies, cybersecurity, software acquisition, and software lifecycle assurance.

Contact Us

CARNEGIE MELLON UNIVERSITY
SOFTWARE ENGINEERING INSTITUTE
4500 FIFTH AVENUE; PITTSBURGH, PA 15213-2612

sei.cmu.edu
412.268.5800 | 888.201.4479
info@sei.cmu.edu