

# Domain Specific V&V Strategies for Aircraft Applications

Aliki Ott, Tobias Hartmann  
Center for Computing Technology, Safe Systems, University of Bremen  
{tsio,hartmann}@tzi.uni-bremen.de

Keywords: Verification and Validation, Domain Analysis, Structured Reviews,  
Generic Specifications, HybridUML

Developing embedded systems – especially in the avionics domain – is a complex systems engineering task consisting of two separate but tightly coupled sub-processes: the development process and the verification and validation process. In the development process, the system's requirements and design is analysed and specified in various requirement documents and the system and its subcomponents are created. In the verification and validation process, the product is verified and tested against the specified requirements (verification process) and the requirement documents are checked for consistency and completeness (validation process). In contrast to this separation of tasks, the results of the development process are the input for the verification and validation process and thus influence the means in the V&V process.

In this presentation, the authors introduce a novel approach to improve the development, verification and validation processes by providing means for

- generating requirement documents for a specific aircraft based on generic development documents which abstract from aircraft specific variations
- deriving V&V documents for structured reviews, tests, test validation and formal verification based on generic verification and validation documents

As a preparation for these tasks, a domain analysis is performed which extracts the structural and behavioural information from different concrete aircraft specifications in an abstract way. The result are generic documents for development, and verification and validation, i.e. these documents are exclusively domain specific and not aircraft specific.

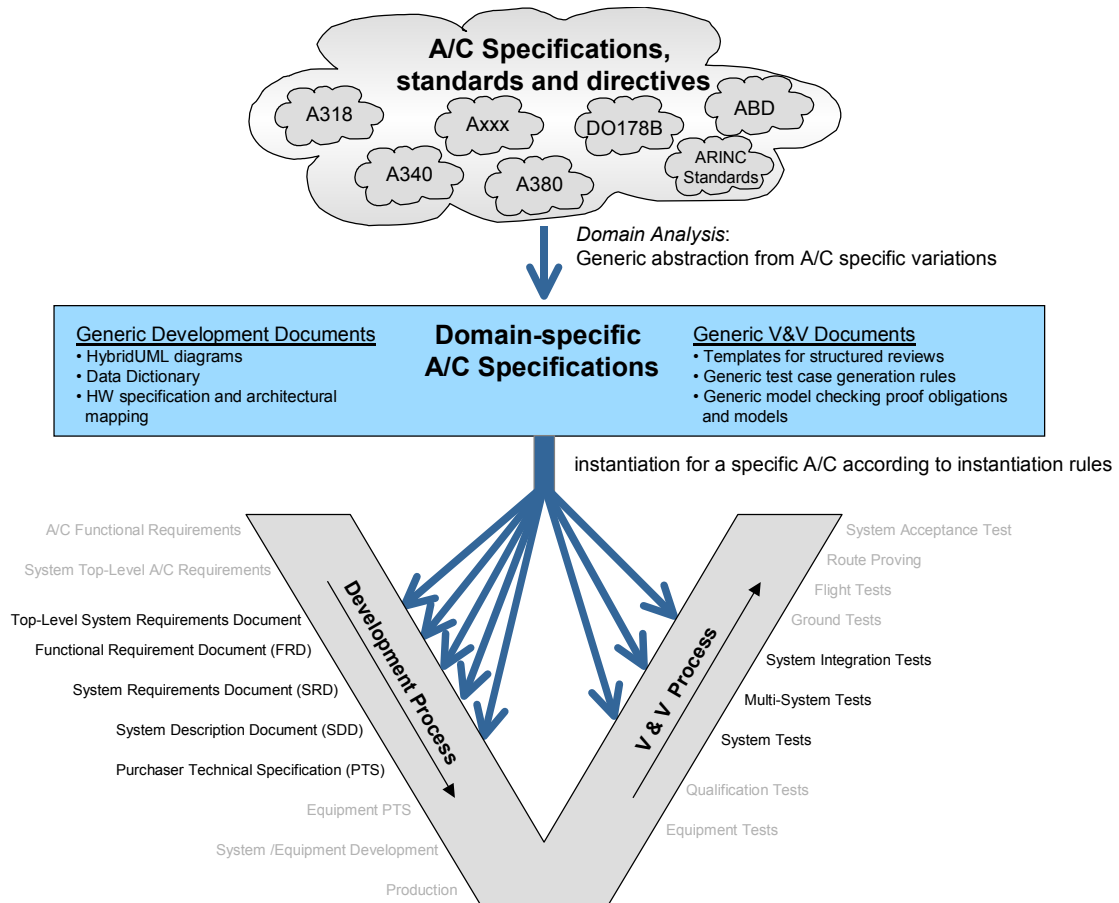
Within the generic specifications, it is – for example – abstracted from the concrete number of peripheral controllers connected to a system controller. Also, for instance, the aircraft-specific smoke detector evaluation function determining alarm situations can be described within a generic model.

The generic development documents are formal specifications consisting of a comprehensive data dictionary, an architectural description and HW information about the system (e.g., mapping of (logical) signals to communication media). The formal specifications are generic structural (i.e., architectural) and behavioural specifications. Analysis of available formal specification techniques with respect to the feasibility for specifying complex real-time system has shown that HybridUML is a suitable formalism: It integrates concepts of hybrid automata into well-known constructs of the UML and thus provides a graphical representation in combination with a formal semantics and extensions for time-discrete and time-continuous behaviour. Further, it provides concepts for hierarchy, parallel composition, separation of concerns and tool support – an important factor for application in large-scale projects.

The above generated domain-specific specifications and templates are a comprehensive knowledge base for improving the verification and validation process of current aircrafts (of which the specifications have been used for the domain analysis) and, in particular, for improving the development and testing of future aircrafts. Both tasks base on aircraft specific instantiation rules which define basically the differences to the generic specification. For example, for the smoke detection system the aircraft specific number and location of smoke detectors or the specific alarm

evaluation function. The result of the instantiation are aircraft specific requirement and design documents – from top-level system requirements to purchaser technical specifications.

The instantiation rules are also used to instantiate the V&V documents for different verification levels – from system tests to ground tests (see figure).



For the structured review templates this means that the generic templates are instantiated according to the verification level and according to the instantiated requirement and design documents. For the test cases generated during the instantiation this means that the generic test case generation rules are applied on the specific formal HybridUML specifications and thus allow automated test data generation using the means provided by HybridUML.

The above described concepts and the format for templates and instantiation rules are currently developed within the research project KATO in collaboration with Airbus Deutschland GmbH. KATO's main objective is the development of new methods, tools and technologies to improve the development and the verification of future aircrafts by providing means for fault avoidance, early fault detection and fault diagnosis. Thus, the aim of KATO is to reduce costs and time for development and verification significantly. HybridUML and the means to execute HybridUML models in hard real-time are developed within the authors' research group [1]. This research has partially been supported by the German Research Council (DFG), project HYBRIS as part of the "DFG-Schwerpunktprogramm – Integration von Techniken der Softwarespezifikation für ingenieurwissenschaftliche Anwendungen" where HybridUML has been applied for train control systems [2].

[1] K. Berkenkötter, S. Bisanz, U. Hannemann, J. Peleska. *HybridUML Profile for UML2.0*. Selected for publication in The International Journal on Software Tools for Technology Transfer, 2005.  
 [2] K. Berkenkötter, S. Bisanz, U. Hannemann, J. Peleska. *Executable HybridUML and its Application to Train Control Systems*. Lecture Notes in Computer Science, 3147:145-173, 2004.