



Pulling the strings

Designing mission and safety critical systems using SysML.

By Matthew Hause.

Mission and safety critical applications require a holistic approach to their design and development and OMG SysML provides the ideal environment.

An extension of UML2, it provides a standard modelling language for engineers to analyse, specify, design and verify complex systems. It enhances systems quality, improves the ability to exchange systems engineering information amongst tools and helps bridge the semantic gap between systems, software and other engineering disciplines.

OMG SysML includes diagrams that can be used to specify system requirements, behaviour, structure and parametric relationships – the four pillars of SysML.

The system structure is represented by block definition diagrams and internal block diagrams. A block definition diagram describes the system hierarchy and system/component classifications.

The internal block diagram describes the internal structure of a system in terms of its parts, ports and connectors. The package diagram is used to organise the model. The behaviour diagrams include the use case, activity, sequence and state machine diagrams. A use case diagram provides a high level description of system functionality, while the activity diagram represents the flow of data and control

between activities. A sequence diagram represents the interaction between collaborating parts of a system, while the state machine diagram describes the state transitions and actions that a system, or its parts, performs in response to events.

Meanwhile, the requirement diagram captures requirements hierarchies and the derivation, satisfaction, verification and refinement relationships, and the parametric diagram represents constraints on system parameter values such as performance, reliability and mass properties to support engineering analysis.

Cross cutting constructs support concerns that cut across the different views and may be addressed by all or disparate parts of the model. These take the form of allocations, requirements and parametrics and apply to both structure and behaviour.

Artisan's OMG SysML Profile not only supports the four pillars of OMG SysML, but also further core OMG SysML elements. Importantly, the implementation allows engineers to work with SysML elements and diagrams as new element types and not just as stereotyped UML types, resulting in faster recognition, better usability and ease of adoption without compromising compliance. OMG SysML artefacts can be deployed on the development of mission and safety critical applications to specify the requirements for solution spaces such as software and hardware to provide both traceability and handover.

Requirements traceability is an essential part of mission and safety critical applications development. With DO-178B, for example, traceability must be provided between system requirements



and high level software requirements, high and low level requirements, low level requirements and tests, tests and code for structural coverage, and from top down and bottom up.

The requirements diagram integrates the system models with text based requirements typically captured in requirements management tools. The UML containment relationship is used to decompose a requirement into its constituent requirements.

More specialised requirement types can be designated using the «requirement» stereotype. Each requirement has an identifier shown next to the id# tag and the text of the requirement is shown in the compartment labelled "txt" in the lower part of the class box. Additionally, requirements and their relationships can be shown on other diagrams.

Tools that provide the functionality to import, export and synchronise requirements and their relationships between the OMG SysML model and an external requirements management tool will allow developers to perform requirements traceability in the tool while taking advantage of the features provided by specialist tools.

A clear description of the system and its environment is essential for mission critical applications. OMG SysML provides block diagrams to support this. The «block» is a general purpose hierarchical structuring mechanism that abstracts away much of the software specific detail implicit in UML structured classes. Blocks can represent any level of the system hierarchy.

An OMG SysML block describes a system as a collection of parts and connections between them that enables communication and other forms of interaction. Ports provide access to the internal structure of a block for use when the object is used within the context of a larger structure. OMG SysML provides standard ports which support client server communication and FlowPorts define flows in or out of a block.

- **Structured diagram types.** Two diagrams are used to describe block relationships. The Block Definition

Diagram (bdd), similar to a traditional class diagram, describes relationships that exist between blocks, while the Internal Block Diagram (ibd) describes block internals. An avionics system bdd, for example, could be represented as a block composed of other blocks, including several processing elements, 24V power and two buses.

Each component has a number of flow ports that describe what can flow in and out. These are connected to compatible ports to enable the required flows.

- **Allocations.** This relationship is used to allocate one model element to another. Allocation is the term used by systems engineers to denote the organised cross association (mapping) of elements within the various structures or hierarchies of a user model. Often, this is the allocation of function to form, such as the deployment of software on a hardware platform.

Allocations can be used as a precursor to more detailed rigorous specifications

Most mission and safety critical applications are developed for military purposes using well defined architectural frameworks like the US Department of Defense Architecture Framework (DoDAF) and the UK Ministry of Defence's Architecture Framework (MODAF). Fortunately, the use of UML, as extended by SysML, as an underlying mechanism for these frameworks has made it feasible to work towards a unified UML/SysML profile for DoDAF/MODAF. The work,



"Mission and safety critical applications require a holistic approach to their design and development." **Matthew Hause**, Artisan Software

and implementations. The allocation relationship can provide an effective way of navigating the model by establishing cross relationships and ensuring the various parts of the model are integrated properly. Integration of software and hardware models means that SIL levels for the various parts can be assigned and verified to ensure a consistent implementation. Hardware/software interfaces can also be verified, as can architectural constraints.

Meanwhile, studies are underway to determine if Goal Structuring Notation (GSN) can be integrated into a model in a similar way as requirements. GSN provides a graphical means of expressing a safety case and creating links from model elements to GSN safety case elements provides direct traceability and the possibility of modular safety cases.

strongly supported by both the DoD and MoD, is being fast tracked through the OMG by the UPDM Group. Draft specification 1.0 has been approved by OMG and is now out for comment pending finalisation.

The extensions made to UML2 in the OMG SysML Profile and the emergence of a unified UPDM Profile provide systems engineers with a robust environment for modelling mission and safety critical systems. At the same time, extensive reuse of UML facilitates a smoother flow down from systems engineering to software engineering than otherwise possible. ■

Author profile:

Matthew Hause is chief consultant at Artisan Software Tools.