The MetaH AADL Toolset

A better way to build hard, real-time, safety critical embedded systems

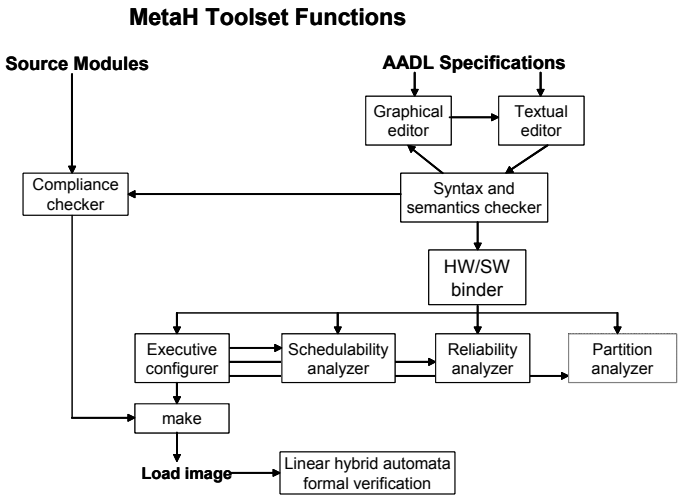
The increasing complexity of embedded systems is driving development of improved architectural modeling and analysis approaches that make building systems faster, less expensive, and more predictable. Honeywell's MetaH was the first comprehensive toolset to tackle the issues of integrated modeling, analysis, system integration and verification. Today, MetaH is both the foundation of the SAE AADL (Architecture Analysis and Design Language)—an emerging standard language for specifying embedded computer system architectures including both functional and non-functional behaviors and properties—and the primary AADL toolset. It accepts specifications written in AADL and performs a variety of verification, modeling, analysis, and code generation activities.

AADL allows the architecture of a real-time, safety-critical embedded system to be specified as an assembly of communicating components, where component functional interfaces and timing and safety behaviors and properties can be precisely defined. MetaH includes tools to perform schedulability analysis, reliability analysis, partition isolation analysis, and compliance checking of source code against AADL specifications. MetaH also automatically configures a middleware layer integrating all components, and generates and verifies a hybrid automata model of core middleware scheduling and security code.

Benefits of Using the MetaH AADL Toolset

Significantly decreases development cost and schedule due to:

- Automation of many system engineering tasks including modeling, implementation, and verification
- Increased assurance that the implementation will behave the way the analyses say it will
- Improved quality and optimality of system design through more accurate and rapid design-time evaluation
- Improved defect avoidance
- Minimization of system hardware resource needs
- Easy, fast, and accurate performance modeling and analysis



The MetaH AADL toolset provides integrated and traceable specification, analysis, implementation and verification. The toolset accepts AADL specifications for hard real-time, safety-critical embedded systems. The tools support system performance modeling and analysis, system integration, and integration code verification.

AADL Specifications—In both graphical and textual format, and fully translatable one into the other, AADL specifications are hierarchical, allow separate component type and component implementation declarations. Semantics cover structural and functional properties and behaviors as well as timing and error and system safety properties and behaviors.

Compliance checker—performs consistency checks between specification and application software components that are being integrated into the system.

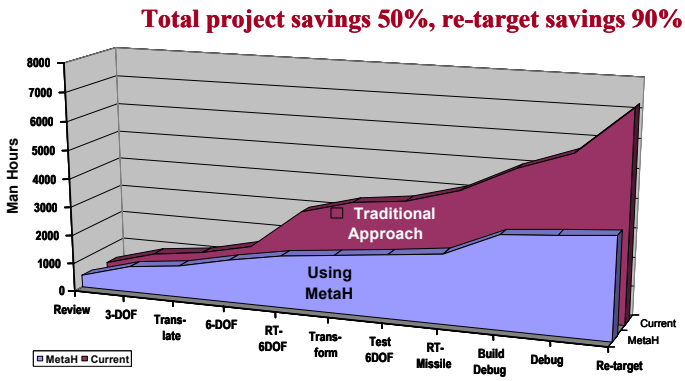
Binder—allocates processes to processors, connections to busses and shared packages to shared memories, ensuring that loads are balanced, utilization thresholds respected, route distances minimal, and memory is appropriately addressable.

Executive configurer—automatically configures a lightweight and efficient middleware to integrate the components of the system.

Make—the make tool performs the compiles and links needed to form executable load images for all processors.

Automata model—formally verifies several timing and safety properties of the middleware.

AMCOM Project Savings



MetaH is proven efficient and effective. Total savings on the Army's AMCOM project were more than 50% over the traditional systems engineering approach.

Analysis Results of Several Primary MetaH Tools

Schedulability Analysis	Reliability Analysis	Partition Analyzer
An exact schedul-ability analysis for each processor and bus in every possible operating mode and exe-cution time sensitivity analysis information	Automatically generates fault tree or Markov chain models for reliability analysis	Verifies that time and space parti-tioning are properly used to enforce assigned component safety/criticality levels

One of the primary goals of MetaH is to couple formal modeling and implementation as closely as possible to increase the accuracy and assurance of analysis results.

MetaH—More than a Traditional CASE Tool or RTOS

MetaH focuses on software and system integration. MetaH can be used with multiple specialized tools (MATRIX®, MatLab/BEACON®, reengineering tools, traditional CASE tools) for detailed component and algorithm design and coding.

MetaH provides semantics for timing, faults and errors, dynamic reconfiguration, safety and security partitioning, and software/software and software/hardware interfacing.

MetaH supports formal modeling and analysis as well as implementation, integrated support from early design through systems integration to verification of high-assurance systems.

MetaH is designed for easy retargeting to a variety of avionics real-time execution environments.

MetaH automatically tailors a system executive for each application, resulting in systems that are smaller, faster, and easier to change and verify.

For further information contact:

Steve Vestal
(612) 951-7049
steve.vestal@honeywell.com

This work has been supported by DARPA (DSSA EDCS and DASADA—DAAH01-00-C-R226, contracts), Army AMCOM,and Honeywell Laboratories

Honeywell

Honeywell Laboratories
3660 Technology Drive
Minneapolis, MN 55418