

# Safety Critical Solutions

As computer control becomes more and more prevalent in all aspects of everyday life, software systems take on increasing

importance. Financial systems depend on software for accounting services and money transfer.

Transportation systems rely on software for control of vehicles and infrastructure. Hospitals depend on software for managing patient records and controlling life-support systems. In the late 1980s, six people died due to the software failure of a computer controlled radiation treatment system. It is clear that the safety of much human life and property now depends directly or indirectly on safe, reliable software.

Software can provide users with considerable flexibility; however, this very flexibility brings with it a

greatly increased chance of error-induced system failure. There is now a growing awareness that strict control is needed to reduce errors in software that is critical to human life and property.

## Aonix: Bringing Safety to Real-Time Systems

- Supplier of industrial-strength development solutions for over 15 years
- ObjectAda™ Real-Time toolset speeds hard real-time development projects
- RAVEN™ Real-Time kernel designed to meet safety-critical and hard real-time requirements
- Embedded projects of any size or complexity serviced by scalable packaged solutions through the entire lifecycle
- Certification expertise and Professional Services personnel to help with your toughest development challenge





*“Companies are now obliged to guarantee that systems they have produced do not violate safety requirements.”*

### Designing and Developing Safety-Critical Applications

The ability to provide solutions for all phases of a project's lifecycle is one of Aonix's key strengths. Beginning with the ability to express the initial system requirements pictorially, Aonix's Software through Pictures® (StP®) modeling tool can go a long way toward speeding up the analysis and design of applications. StP automatically generates source code from graphical models for further refinement at the development level with Aonix's ObjectAda™ development environment.

ObjectAda Real-Time RAVEN™ provides a complete Integrated Development Environment (IDE) to accommodate the most demanding development requirements. Comprised of an efficient cross-compilation system, high-performance code generator, a visual tool (perfoRMAx™) to help schedulability analysis, source-level debug facility, target

download support, and the fast RAVEN execution environment, ObjectAda delivers the best value for critical systems development projects. Additionally, ObjectAda uniquely supports safety-critical application development by use of pragma\_restrictions that identify “unsafe” constructs during compilation as they apply to the runtime design. Pragma\_restrictions are defined by the Ada 95 standard so their use doesn't circumvent correct Ada 95 programming styles.

### Multi-language Development Support

Very often, in a complete system, some components may not be required to meet the highest levels of criticality. Thus portion of the application could be developed using another language such as C/C++ or Java. The Aonix solution supports multiple languages in all phases of the system-development lifecycle.

### System Verification and Testing

A variety of verification and testing strategies must be used to achieve confidence in a safety-critical system. One aspect of testing is to assure the final implementation of an application meets the expectations of the original design. Aonix supports the automation of this kind of testing with Validator/Req™, a testing solution that generates tests directly from system specification. This delivers a thread of proof from the original requirements through the design and development phases and into the test phase of the project.

Another goal of a specification-based testing strategy is to adequately check the behavior of the completed system. Each function must be tested with typical data values and also with data values that check the most extreme conditions that could be encountered by the system. The tests and testing environment must be designed to ensure that the software is as close to the final configuration as possible and that all the requirements are thoroughly tested. All derived requirements, such as initialization of the stack or set-up of memory-addressing registers, must also be tested. To comply with certification criteria at the highest criticality level, every byte of code must be executed and every branch must be covered for both conditions. Aonix provides a tool, AdaCover, to help satisfy this requirement. AdaCover is qualified for showing certifiability of any safety-critical application.

#### Ada Language Use in Safety-Critical Systems

Ada is a general-purpose language that contains a number of features that should not be used in safety-critical applications. Most general-purpose Ada solutions don't restrict operations that potentially allow problematic conditions such as memory fragmentation and certain tasking operations, which by their nature are non-deterministic and inappropriate for systems with highly-critical requirements.

#### ObjectAda Real-Time RAVEN: The Aonix Solution

The Aonix real-time kernel, RAVEN, is designed on the Ada 95 tasking restrictions set as defined in the *RAVENSCAR Profile*. Adopted at the Eighth International Real-Time Ada Workshop (IRTAW-8),

##### Ada: The Ideal Foundation

Ada has numerous properties that make it the natural choice for the development of safety critical systems.

- Ada is an ISO standard
- Ada supports object-oriented design and programming
- Ada has a legible style to facilitate reviews and maintenance
- Ada has a coherent, modular construction
- Ada has been designed to detect errors at compile time and execution
- Ada allows the basic elements of the target hardware to be accessed in a logical manner
- Ada limits the features used by a program unit, eliminating unsafe behavior

Ravenscar UK, the profile accommodates certification requirements for high-integrity (safety-critical), real-time systems.

This special Ada 95 tasking model is especially important to safety-critical systems that must be totally bounded in time and memory usage. With ObjectAda Real-Time RAVEN, the time taken to

execute and the amount of memory used by each element of the program can be determined and verified for certification.

#### Designed to Address Safety-Critical Systems:

From the start, the design and implementation of RAVEN is focused on deterministic behavior, which is a requirement for safety-critical systems. As a result, RAVEN satisfies the highest levels of criticality including Level A as defined in the DO-178B software safety guidelines and required by the FAA for airborne systems.

#### Certification Option

The ObjectAda Real-Time RAVEN Certification Option supplies customers with all of the lifecycle data for the real-time kernel needed to meet the certification requirements of standards like DO-178B for avionics, IEC 1508 for industrial, and RIA-23 for rail to just name a few. For example, to satisfy the requirements of DO-178B, the Certification Option includes:

- RAVEN kernel source code
- A design document describing the structure and components of RAVEN
- Primary requirements documentation derived from the Ada 95 standard
- Derived requirements based on the Aonix product design for RAVEN and compilation system design

# Safety Critical Solutions

- A set of tests for functional testing of primary and derived requirement with scripts and reference listings for a “standard target”
- The AdaCover tool for performing coverage testing at the machine-code level
- A set of tests for coverage testing of primary and derived requirements with scripts and reference listings for a “standard target” and the supporting coverage analysis
- Configuration Management, Quality Verification, and Software Development plans
- Design, code, and requirements standards
- A complete matrix that maps each module of the Aonix-supplied source code to the primary and derived requirements
- Quality assurance records, configuration management records, and a software accomplishments summary showing compliance with the regulatory requirements for certification

Aonix also warrants the certifiability of RAVEN. This feature of our Certification Option is a significant benefit to your development staff during the riskiest phase of their development cycle. Our safety-critical and real-time professional services experts are here to help you with any certification issues you might encounter.



## The Safety Imperative

The era of safety-critical software is just beginning. Software applications will increase in size and complexity as the move toward automated systems continues to grow in all sectors. Public expectations for safety in products and services will also increase and a growing number of industries will be forced to develop and enforce their own safety-critical standards.

Every company developing software for safety-critical applications must prepare itself to meet the challenges of certification resulting in a number of positive benefits to the enterprise.

- Products and services will be safer and more reliable
- Catastrophic financial liabilities resulting from lawsuits and product failures or recalls can be minimized
- The market advantage of using “certified” or assured software can result in greater profitability

*“Every company developing software for safety-critical applications must prepare itself to meet the challenges of certification...”*

# Safety Critical Solutions

## Safety Critical Standards

Recent legislation has produced a number of directives designed to ensure safety. Companies are now obliged to guarantee that systems they have produced do not violate safety requirements. Even company directors can now be held personally liable for loss of life or property resulting directly or indirectly from unsafe software installed, sold, or included as part of a product sold by their company.

Most industries, including transportation, nuclear energy, and medicine are in the process of setting—or have already set specific standards for the development, testing and certification of safety-critical software. As these standards emerge, the focus is on the use of best practices. In some areas, standards mandate specific techniques for the development of safety-critical systems. In all cases, a reasoned justification for the techniques actually used is required.

## The Avionics Example

The avionics industry has historically taken the lead in development of safety-critical systems. Before an airplane may carry fare-paying passengers, it must undergo a thorough certification process. Each component of the airplane is assigned a criticality level commensurate with the effect its failure would have on the safety of passengers. The confidence in each component must match the adverse



effect that the component would have should it fail. Since many of the components of an airplane are software-controlled, overall safety is critically dependent on the accuracy of the embedded software.

The combined efforts of several government agencies have resulted in publication of DO-178B as the standard guidance document that provides for the certification of software used in airborne systems and components. An area of key importance is the software language used for the final installed system. Standards specify that the language must be well-defined, have validated tools, enable modular programming, have strong checking properties, and be clearly readable. Of all the programming languages widely available today, Ada provides the best baseline for these safety-critical systems.

## Certification: The FAA DO-178B Scenario

When software has been written to match its requirements and specification, has been fully tested and documented, and includes verification materials to show compliance with the requirements of a safety standard, it is deemed to be "certifiable." The avionics industry requires that safety critical software be certified according to strict United States Federal Aviation Administration (FAA) and Europe Joint Aviation Authority (JAA) guidelines before it may be used on any commercial airliner. Other industries are in the process of mandating their own certification standards for safety critical systems. Aonix provides developers of safety critical software with a cost-effective solution to application certification.

**Aonix — A World Leader in  
Software Engineering Solutions**

Aonix has been supplying safety-critical solutions for over a decade, beginning with its first DO-178B certifiable kernel, C-SMART™. As a result, Aonix is uniquely qualified to provide the software engineering tools needed to meet the challenge of software-safety assurance. Since the early days when Aonix first created Ada compilers and software engineering modeling tools, the company has been firmly committed to highly reliable development software.

This commitment led naturally to the production of software-engineering tools for safety-critical applications that have helped minimize the significant risks often

associated with developing safe applications to customers around the world.

Building on this tremendous expertise and long-term experience, Aonix is now helping customers successfully certify and deploy systems developed with the same proven methods and powerful tools but with the latest safety-critical technology. Aonix and RAVEN—THE complete, cost-effective safety-critical solution.

Aonix remains at the forefront of software engineering development with products that comply with international standards and a proven dedication to quality Aonix has the tools you need today, and the vision to help you build tomorrow's competitive software systems.



To obtain more information, please contact Aonix at [www.aonix.com](http://www.aonix.com) or your local Aonix office.

**Aonix World Headquarters**

Phone: (800) 97-AONIX  
Fax: (619) 824-0212  
E-mail: [info@aonix.com](mailto:info@aonix.com)



**United Kingdom**

Phone: +44 (0) 1491 579090  
Fax: +44 (0) 1491 571866  
E-mail: [info@aonix.co.uk](mailto:info@aonix.co.uk)

**Karlsruhe, Germany**

Phone: +49 (0) 7 21/9 86 53 - 0  
Fax: +49 (0) 7 21/9 86 53 - 98  
E-mail: [info@aonix.de](mailto:info@aonix.de)

**München, Germany**

Phone: +49 (0) 89/45 10 57 - 0  
Fax: +49 (0) 89/45 10 57 - 30  
E-mail: [info@aonix.de](mailto:info@aonix.de)

**France**

Phone: +33 (0) 1 41 48 10 00  
Fax: +33 (0) 1 41 48 10 20  
E-mail: [info@fr.aonix.com](mailto:info@fr.aonix.com)

**Sweden**

Phone: +46 (0) 8 601 9491  
Fax: +46 (0) 8 601 9499  
E-mail: [info@aonix.se](mailto:info@aonix.se)