WHITEPAPER

Saving Millions of Dollars in the Development and Certification of Safety-Critical Applications

Executive Summary

As electronics systems complexity has risen, so has the importance of the communications infrastructure. Besides the inherent challenges throughout the design, development, and integration phases, safety-critical systems have the added complexities and costs relating to certification. Fortunately, certifiable middleware offers an extremely cost-effective alternative.

In this white paper, certifiable communications middleware is overviewed within the context of a specific safety-critical application: unmanned aerial vehicles (UAVs). Actual UAV use cases have proven that certifiable communications middleware can deliver cost savings in the range of $2 million. Equivalent savings are realistic for any project that must meet stringent safety-certification criteria. The certification evidence for middleware solutions is also highly re-usable, which translates into excellent long-term savings and value.

Safety-Critical Applications

The design of modern Unmanned Aircraft Systems (UAS) includes many safety-critical components such as processors, operating systems, communication infrastructure, and application software. The integration of UAS in the National Airspace System is starting to put more weight on implementation of safety-certification guidelines such as DO-178C, making the design of these systems even more demanding.

The development challenges relating to UAS apply to a broad range of safety-certifiable applications. Similarly, the design challenges in the fields of defense-related Unmanned Arial Vehicles (UAVs) and avionics apply across many commercial industries such as automotive, medical, industrial automation, and more.

Increasing Level of Sophistication

Modern UAS are no longer a simple combination of one Ground Control Station (GCS) and one UAV fulfilling one mission requirement. Instead, these systems will be networks of multiple UAVs from different vendors, carrying configurable payloads, and multiple GCSs from a variety of system integrators. All of these components interoperate to achieve multiple and varying mission objectives.

The challenge will be to ensure that data and capabilities of smart sensors onboard UAV payloads are accessible to every relevant participant in the environment. For example, target data extrapolated by an onboard sensor from a UAV video stream may need to be shared with any number of combat systems. Sharing can take place over any one of a number of different communication links in real time.

Communication Challenges

The efficient use of the available communication infrastructure plays a key role in UAV design. As system complexity has increased, communications infrastructure has not advanced in pace with processor technology.

To compensate, smart sensors have emerged and operate more autonomously. Only the most important information gets passed to in-field personnel (to conserve bandwidth), but this mission-critical data must be exceptionally reliable. This applies to air-to-ground data links as well as to networks and busses onboard bigger airframes and high-speed networks in the GCSs.

With the increased military requirements for interoperability between UAVs and their payloads (i.e., smart sensors) and GCSs, the point-to-point communications solutions of the past cannot meet the needs for these highly distributed and complex systems.

Communications Within a "System-of-Systems" Architecture

Today's UAVs require a communication infrastructure that supports any-to-any endpoint connections, whether within a single system or within the larger deployment. The challenge is to design a UAS around a communications infrastructure that spans the entire UAS, from onboard the vehicle, down to the GCS, and between subsystems in the GCS.

What are the fundamental requirements for such a flexible communications infrastructure?

- It must be based on open standards, to maximize interoperability between multi-vendor systems.
- It must be architected as a true peer-to-peer framework, with no single point of failure (i.e. a central server) or performance bottleneck.
- It must be portable to the various communication media used in a UAS, such as radio links between UAVs and GCSs and high-speed networks such as 10Gig Ethernet in the GCSs.
- It must be available on heterogeneous computer platforms:
  - GCSs are predominantly built upon mainstream OSs such as Linux and Windows on mainstream CPUs such as Intel x86.
  - UAVs tend to be built on embedded processors such as ARM and PowerPC, in memory-constrained environments running specialized OS environments such as platforms based on ARINC 653 or MILS.

With the integration of UAS in National Airspace System, safety certification is also becoming a requirement. Therefore, a communications infrastructure for UAVs must be a certifiable component, meeting guidelines such as those specified by DO-178C, in addition to meeting the above requirements.

DDS: A Proven Platform

With the exception of meeting the safety-certification requirement, a communication infrastructure that meets all fundamental requirements already exists. Object Management Group (OMG) publishes the Data Distribution Service (DDS) standard, which was initiated in 2001 by a consortium including RTI and various systems integrators. RTI introduced the first commercial implementation of DDS in 2005.

At its core, DDS implements a real-time data bus based on a connectionless architecture. This architecture overcomes problems associated with point-to-point system integration, such as lack of scalability, interoperability, and the ability to evolve the architecture.

DDS implements connectionless architecture by categorizing applications as publishers (i.e., providers) of data, or subscribers of data (i.e., consumers of data). A DDS-based system has no hard-coded interactions between applications; all communications occur over the common data bus.

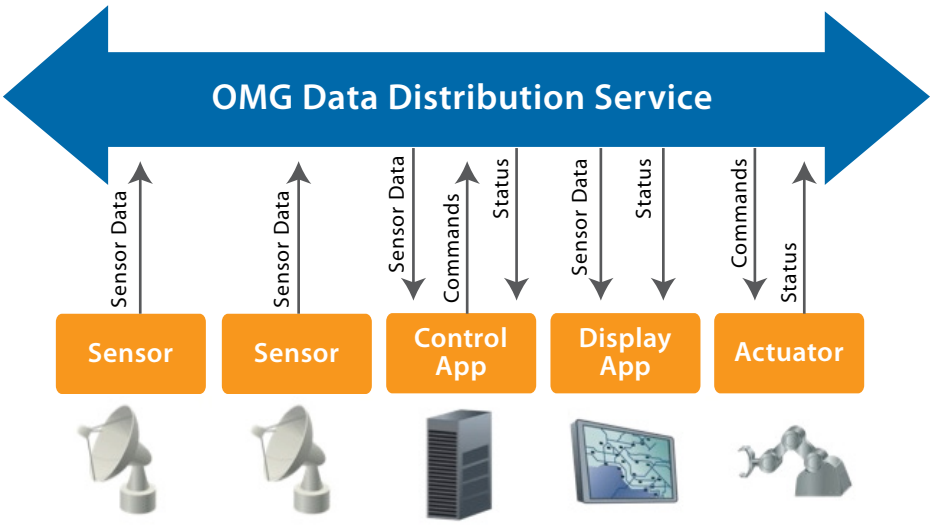

Figure 1. DDS peer-to-peer real-time Data Bus.

The data bus automatically discovers and connects publishing and subscribing applications (see Figure 1). For example, no changes are required with the addition of new sensors. Active sensors can publish data that might include radar data or infrared camera images. Other applications, such as a control application or a tactical display, subscribe to the real-time sensor data. The control application can process the data and invoke appropriate navigation changes, for example, or publish results to its own subscribers such as down in a GCS.

This example shows how DDS communication platforms can deliver on-demand connectivity as run-time services. No hard-coded connections are designed into the UAV and GCSs.

DDS for Safety-Critical Applications

General-purpose DDS is being used in hundreds of applications and systems across many industries including medical, energy, mining, air traffic control, automotive, unmanned systems, industrial SCADA, naval systems, and air and missile defense. These systems tend to process high-volume and highly frequent updates, like sensor information, and accurate transmissions are critical. The implications of system failure are often severe, leading to loss of property or even loss of life.

The proven success of DDS makes it an excellent starting point for safety-critical applications such as UAV systems.

The Certification Challenge

Certification is expensive. A DO-178C certification process is carried out for the entire aircraft or an entire system. Components, such as on-board software, cannot be separately certified. However, each component can be certifiable. This means the software comes packaged with certification evidence (test results and documentation) that can be used during actual certification of the host aircraft or system.

For DO-178C, costs can range from $50 to $100 per executable line of code (ELOC), depending on the certification level[1]. These are the costs for creating the certification evidence only and do not include the costs for designing and writing the code.

Certification for DO-178C requires that all objectives be fully met. Level A includes 71 objectives; Level B includes 69. All steps must be documented in detail.

[1] DO-178C Safety Levels range from E (no serious safety issues) up to A (catastrophic impact, which may include total loss of an aircraft).

Certification testing for software encompasses three categories for DO-178C:

- Statement Coverage (SC), where every statement is invoked at least once during testing (basic code coverage)
- Decision Coverage (DC), where every point of entry and exit is exercised at least once during testing and every decision in the code is tested both true and false
- Modified Condition Decision Coverage (MCDC), where additionally each condition in a decision is tested to independently affect the decision's outcome

Tools are available to automate code coverage, but this overview for DO-178C illustrates why certification costs have risen to the above-stated levels.

The DO-178C objectives dictate that code be developed with extraordinary attention paid to testability. Code must be deterministic, to enable repeatable test results. Dead code must also be diligently identified and eliminated.

Deterministic Code

Testing must be deterministic, meaning that code must be designed to consistently yield the same behavior every time with no side effects. Dynamic memory allocation exemplifies a source of non-determinism. Dynamic allocation can lead to memory fragmentation. This requires the operating system to sporadically compact memory, which is a source of non-determinism.

A Safety-Certifiable DDS Platform

Since safety certification is costly and developing safety-certifiable software comes with its additional set of unique challenges, mission-critical components such as communication middleware must be developed with minimum line count, testability, and determinism as the dominant requirements.

The minimum profile of the DDS specification can be further stripped down to match the code size of a safety-certifiable component. Eliminating non-essential general-purpose communication capabilities can significantly lower certification costs.

How do these considerations affect the implementation of a DO-178C Level A certifiable communication platform? Adjustments must be made:

- **A subset of DDS features** is necessary to reduce line count. A certifiable DDS implementation should only include core capabilities that are relevant in safety-critical systems. For example, standard DDS supports the creation of logical network partitions at run-time. Avionics systems will not typically require this kind of dynamic behavior, and it can therefore be stripped out to simplify system certification.
- All sources of **non-determinism must be eliminated**. There is no dynamic memory allocation after system initialization. This means applications are preconfigured with their required resources.
- **Simpler data structures and algorithms** can speed performance and lower code size. They also enable limiting of the size of an on-board system. Larger off-board systems can be integrated through a bridge that connects to any implementation that requires the full DDS feature set.

A Certifiable DDS Solution

The previous lists of features and best practices stem from lessons learned by the RTI team during the company's years as a DDS pioneer and solution provider. RTI Connext DDS Cert, the company's certifiable DDS solution, tracks the OMG specifications for DDS including wire protocol RTPS compatibility and seamless integration with other general-purpose DDS implementations.

A DDS Subset

Implemented as a subset of the standard DDS minimum profile, the Connext DDS Cert middleware includes:

- Support for multiple DDS domains, for network partitioning, which is important for mixed-criticality applications
- Ability to create all basic DDS objects and entities (domain participant, publishers, and subscribers) and keyed and keyless topics

- Periodic polling for input by subscribing applications as well as notification of data arrival
- Data reading and caching options for applications, such as read and leave in cache or take data and remove from cache
- Data publishing options for applications, such as publishing with system or application-set timestamp
- Ability to dispose of stale data
- Bandwidth-efficient heart-beating mechanisms to periodically announce subsystem availability
- Thread-safe code

Memory Management

Since certification requires deterministic code, the standard dynamic memory-allocation scheme of general-purpose DDS is problematic for safety-critical applications. Instead, Connext DDS Cert middleware implements a deterministic memory-usage model.

All resource limits are configured before creating entities. Memory is only allocated during these create operations, during system setup and initialization. After that, the middleware enforces static memory (no growth).

Quality of Service (QoS) Parameters

Resource limits are configured using standard DDS QoS parameters. The DDS standard also includes other types of QoS parameters that are applicable to safety-critical applications and certification and are therefore included in the certifiable implementation.

- Reliability QoS: Protocol parameters allow a choice of best-effort or reliable communications. Most safety-critical applications use reliable communications (with the associated repair traffic), while others need best-effort communications, specifically when processing highly frequent updates, to avoid any interference between data traffic and repair traffic.
- Durability QoS: These settings can help avoid complexities with startup sequences between subsystems, for example. It also supports bringing devices online or taking them offline during operation. After a publisher has sent data, any entity that joins later can be configured to automatically receive historic data. If configured this way, the publisher will resend the latest data to late joiners.
- Ownership and strength QoS: Applications can manage redundancy with these QoS parameters and allow the middleware to automatically filter duplicates.

Certifiable Discovery

The full dynamic discovery protocol implemented by the general-purpose DDS standard has been replaced with a modified quasi-static discovery protocol. The first stage of discovery – participant discovery – remains the same as standard DDS.

The second stage of discovery for certifiable DDS differs completely. Rather than discovering publications and subscriptions dynamically over the network, a static configuration is loaded from a file. As a result, only predefined components and interfaces will connect on the network.

RTI Certification Evidence

The RTI Connext DDS Cert code base, derived from Connext DDS Micro, is available today. Certification evidence is being developed and will be available within a year.

When released, the RTI certification test results will be delivered on a DVD. Included will be the complete evidence set: all required documents, high-level and low-level requirements with full traceability, architectural design description, and hyperlinked cross-references for easy access.

Comprehensive – and Repeatable – Cost Savings

Program teams can take advantage of a certifiable DDS implementation such as RTI Connext DDS Cert and eliminate the costs, time, and risks associated with in-house development. The reduced code size and targeted DDS feature set meet the needs of a broad range of safety-critical applications (e.g. UAVs and GCS systems).

Besides lowering software development costs, certifiable communication middleware also notably reduces

certification costs. These can conservatively add up to $2-million for just the certification evidence of the communication middleware:

Executable lines of code, communication middleware:	20,000
Certification costs, DO-178C Level A:	$100/ELOC
TOTAL COST, certifiable communication infrastructure:	$2,000,000

The certifiable DDS implementation from RTI consists of approximately 25,000 ELOC. For the DO-178C Level A objectives, this represents a cost of $2,500,000. The certification evidence that will be offered by RTI will be available at only a fraction of this cost – and will be re-usable.

Certifiable DDS is a subset of full DDS with a reduced feature set tailored to safety-critical applications. It is therefore unlikely that any application-specific communication infrastructure can be developed in less lines of code. But even with a significantly reduced feature set at just 10,000 ELOC, the cost savings by using Connext DDS Cert are still significant.

Lastly, the elimination of risks associated with certification is another major benefit of a solution such as Connext DDS Cert. With positive test results in hand, at the beginning of the project, teams can have confidence that the communication infrastructure requirements have been satisfied.

To Learn More

For more information about the full RTI Connext DDS platform and related integration best practices, download these RTI white papers:

- Best-Practices Data-Centric Programming: Using DDS to Integrate Real-World Systems
- Repeat Success, Not Mistakes; Use DDS Best Practices to Design Your Complex Distributed Systems

Visit the RTI website to read more about RTI Connext DDS Cert.

Download a free trial of the full RTI Connext DDS solution.

About Real-Time Innovations

RTI is the world leader in fast, scalable communications software that addresses the challenges of building and integrating real-time operational systems. RTI Connext solutions meet the needs of enterprise-wide integration—from the operational edge to the enterprise data center. The RTI standards-based software infrastructure improves the efficiency of operational systems while facilitating better decisions, actions and outcomes for the business enterprise.

For over ten years, RTI has delivered industry-leading products and solutions for customers in markets ranging from Aerospace & Defense, Process Automation, Financial Services, Energy, Automotive, Health Sciences and Transportation Management.

Founded in 1991, RTI is privately held and headquartered in Sunnyvale, California.

rti
Your systems. Working as one

CORPORATE HEADQUARTERS
232 E. Java Drive
Sunnyvale, CA 94089

Tel: +1 (408) 990-7400
Fax: +1 (408) 990-7402
info@rti.com

www.rti.com