Using Industry Standards to Accelerate Adoption of Next-Generation Autonomous Platforms

eVTOL Writers Group Interview
24 March 2021

Chip Downing
Senior Market Development Director, Aerospace & Defense, Real-Time Innovations, Inc.
Chair, Future Airborne Capability Environment (FACE) Outreach Team
Agenda

• Quick Introduction
• RTCA DO-178C Standard
• FACE Avionics Standard
• DDS Connectivity Standard
• Integrating DO-178C, FACE, and DDS
• Q & A
Corporate Overview

Leader in Software Connectivity Frameworks for Autonomous Systems including Mission-Critical A&D Systems

• HQs in Silicon Valley with worldwide offices
• 1,500+ commercial designs
• 600+ research projects
• Leader in Data Distribution Service (DDS)
• Annual revenue growth of 25%+
250+ RTI Autonomous Vehicle Programs!

• 50+ commercial systems
  – 10+ Passenger vehicles
  – 10+ EV startups
  – 5+ Software platforms
  – 8+ Trucks, mining vehicles, forklifts
  – 2 Flying taxi services
  – 2 Hyperloop and other
  – 2+ Autonomous ships
  – 2+ Underwater robots

• 100+ defense systems (land, sea, air)

• 75+ research programs
  (companies, universities, etc.)
Indy Autonomous Challenge

Dalarra IL-15

Level 4 Autonomy
Near 200 mph

Over 30 teams
Over 500 students
Over 35 universities

https://www.indyautonomouschallenge.com/
Considerations
• Safety
• Security
• Regulatory
• Political
• Technical
• Financial
• Educational
• Operational
RTCA DO-178C Safety Standard
RTCA DO-178C and EUROCAE ED-12C Standard

- Developed jointly by RTCA and EUROCAE
- Is an assurance standard, and not a development standard
- Development outcomes need to satisfy the assurance criteria of DO-178C in the areas of planning, requirements definition, design and coding, integration, verification, configuration management, and quality assurance
- Regulatory compliance for software can be shown by conforming to the guidelines described in RTCA DO-178C
Certification Standards for Airborne Systems

- As part of aircraft certification, applicant defines the product, establishes its regulatory requirements that apply to the product, and demonstrates that those requirements have been met.
- Aircraft and Jet Engines are certified as systems
  - Individual aircraft components and software cannot be certified
  - Evidence for all software components are offered as part of the aircraft certification process.
- DO-178C standard is used to assure safety of avionics software
- Evaluated by FAA Designated Engineering Representatives (DERs)
Design Assurance Level Determines Rigor Needed for Compliance

- DO-178C mandates Design Assurance Level (DAL) be identified for each avionics system corresponding to hazard classifications derived from the safety assessment.
- DAL Level defines the rigor (number of objectives) necessary to demonstrate compliance.
- Level A assigned to software with catastrophic failure conditions, whereas Level E is assigned to software with no safety-related failure effects.
- The FAA requires a minimum of Level D compliance for any aircraft takeoff-required avionics software (e.g. flight data recorder software).

- Examples:
  - Level A – Primary flight control systems
  - Level E – Passenger entertainment software

DO-178C Levels and Objectives

0 (just prove you are Level E)

LEVEL A: 71 Objectives
LEVEL B: 69 Objectives
LEVEL C: 62 Objectives
LEVEL D: 26 Objectives
LEVEL E: 0 Objectives (just prove you are Level E)
RTCA DO-330 and EUROCAE ED-215

Software Tool Qualification Considerations

• **RTCA DO-330 and EUROCAE ED-215** provide tool qualification guidance for building airborne and ground-based software that are achieving safety certification using RTCA DO-178C, DO-254, and DO-278 safety certification guidance.

• DO-330 is an expansion of FAA Order 8110.49 Chapter 9 under DO-178B that described tool verifications
  - Design Tools – modeling tools, code generation tools, compilers, and linkers
  - Verification Tools – structural coverage tools, code analysis tools, testing tools

• DO-330 describes 5 Tool Qualification Levels (TQL) categories
  » TQL-1 to TQL-5, TQL-1 is the highest level, TQL-5 is the least rigorous
DO-330 Certification Tool Providers

- **AdaCore** [Ada Solutions]
- **Ansys** [Design Tools]
- **DDC-I** [RTOS]
- **LDRA** [Test Tools]
- **Presagis** [Graphics]
- **Rapita Systems** [Test Tools]
- **The Mathworks** [Design Tools]
- **Vector** [Test Tools]
- **Verocel** [Cert Tools]
- **Wind River** [RTOS]
- **WolfSSL** [Security]
FACE Approach

Develop a Technical Standard for a software Common Operating Environment (COE) designed to promote portability and create software product lines across the military aviation domain.

Aspects of the FACE Approach:

• Business processes to adjust procurement and incentivize industry
• Technical practices to promote development of reusable software components
• A software standard to promote the development of portable components between differing avionics architectures
FACE Standard-of-Standards

- Ada 95
- ARINC 661
- ARINC 739
- C
- C++
- ARINC 664
- ARINC 653
- IDL
- IPv6
- POSIX
- 1553
- Java
- UDDI
- OSGi
- XML
- OpenGL
FACE Operating Systems Segment (OSS)
Common Services and Portable Components reside here

FACE Portable Components Segment (PCS)

FACE Transport Services Segment (TSS)
All communication, including inter-Up communication, is achieved through message-based transport middleware which reside in this segment

FACE Platform-Specific Services Segment (PSSS)
Standardized Up-level data products and indirect hardware access are provided by this segment

FACE I/O Services Segment (IOSS)
Standardized, but indirect hardware access is provided in this segment

FACE Operating Systems Segment (OSS)

Language
Run-time

Graphics
Drivers

Hardware
Device Drivers

Hardware, Microprocessors, Devices, Boards
FACE Conformance Program
Steps and Processes

Software Supplier

Conduct Preparation

Initiate Verification

Initiate Certification

Initiate Registration

FACE Verification Authority (VA)

FACE Certification Authority (CA)

FACE Library Administrator (LA)

FACE Verification
The process of determining the conformance of an implementation to specification requirements. The VA consist of technical expert(s) on the FACE Technical Standard and Verification process and approved by the FACE Consortium Steering Committee.

FACE Certification
The process of applying for a FACE Conformance Certificate once verification has successfully been completed. Certification is processed through the FACE CA.

FACE Registration
The process of listing FACE Certified UoCs in a public listing of FACE Certified UoCs known as the FACE Registry. The FACE Registry is accessed from the FACE Landing Page.

*The FACE Landing Page can be accessed at [http://opengroup.org/face](http://opengroup.org/face)
FACE Certified Conformant Products Available Now

Now 22 FACE Certified Conformant Products from 13 Different Suppliers in the FACE Registry
Data Distribution Standard (DDS)
DDS: Open Cross-Industry Standard

• Data Distribution Service (DDS) is an open industry standard for data-centric connectivity

• From OMG, the world’s largest systems software standards organization
  – UML, SysML, XMI, CORBA, DDS
  – Industrial Internet Consortium (IIC)

• DDS is open and multi-vendor
  – Open Standard and Open Source
  – 12+ implementations

Interoperability between source written for different vendors

Interoperability between applications running on different implementations

©2021 Real-Time Innovations, Inc.
# Standard Capabilities with Security Plugins

<table>
<thead>
<tr>
<th>Security Plugin</th>
<th>RTI Connext Secure Plugin Description</th>
</tr>
</thead>
</table>
| **Authentication** | - X.509 Public Key Infrastructure (PKI) with pre-configured shared Certificate Authority (CA)  
- RSA or Elliptic Curve Digital Signature Algorithm (ECDSA) for signing, and Diffie Hellman (DH) or Elliptic Curve Diffie-Hellman (ECDH) for key agreement |
| **Access Control** | - Specified via permissions file signed by shared CA  
- Security configuration per Domain, Partition, and Topic  
- Access Control per Domain, Partition, and Topic |
| **Cryptography** | - Automatic/Protected symmetric key distribution  
- AES-128/192/256-GCM for encryption  
- AES-128/192/256-GMAC for message authentication code (MAC)  
- Separate keys per DataWriter and DataReader |
| **Data Tagging** | - Tags specify security metadata, such as classification level  
- Can be used to determine access privileges (via plugin) |
| **Logging** | - Log security events to a file or distribute securely over Connext DDS |
DDS Connectivity Framework for Standards

Data Distribution Service (DDS)
The DDS Layered Databus

Flight Control
Mission Computer

Sensor Bus
Edge Processing

Flight Control Bus

CMS
HMI

Flight Control Computer

©2021 Real-Time Innovations, Inc.
I/ITSEC Joint Demo

Diagram showing the integration of various components and systems, including:
- VT MAK: F-18 HLA Federate, VR-Vantage Stealth
- SimBlocks.io: One World Terrain
- Microsoft Flight Simulator X: FSK to DDS Bridge
- DDS and CIGI Host
- Map Control (LabVIEW)
- FACE TSS

The diagram illustrates the connectivity and integration of these components.
Integrating DO-178C, FACE, and DDS
RTI Connext DDS COTS FAA RTCA DO-178C and EUROCAE ED-12C DAL A Certification Evidence

- Plan for Software Aspects of Certification (PSAC)
- Software Quality Assurance Plan
- Software Configuration Management Plan (SCMP)
- Software Development Plan (SDP)
  - Software requirements standards
  - Software design standards
  - Software coding standards
- Software Verification Plan (SVP)
- Software Requirements Specification (SRS)
- Software Design Document (SDD)
- Certified platform production binary
- Software Life Cycle Environment Configuration Index (SECI)
- Traceability Matrix
- Software Development Folder
  - Design reviews
  - Code reviews
  - Test reviews
  - Functional tests
  - Coverage results (object level)
- Tools Qualification Documents (TQD)
- Software Vulnerability Analysis
- Software Accomplishment Summary (SAS)

Over 5,000 hyperlinked files – in COTS packaging
RTI FACE Commitment

- Over 10 years of FACE Consortium participation
  - TWG TSS
  - TWG Data Model
  - BWG Outreach
- First Certified Conformant FACE 2.1 Transport Service Segment (TSS) 7 Dec 2018
- FACE 3.1 TSS
  - FACE 3.1 Conformance Certification Q2 2021
  - DO-178C DAL A Certification Evidence Q3 2022
Autonomous Sensor-to-Cloud Capabilities

**Public Internet**

- End-User Applications
- Connect with RESTful/Web Sockets

**Fleet Management**

- Traffic Management
  - Traffic Light Control
  - Congestion Management
- Road Management
  - Environmental and Road Conditions

**V2V and V2X**

- Probe Data Collection (Sensors)
- Environmental Weather
- Dynamic Vehicle Location

**In-Vehicle Platform**

- Collision Avoidance
- Navigation
- Safety Certified

**Unified Data Model**

- Cloud Databus
- Site Databus
- Unit Databus
- Machine Databus

©2021 Real-Time Innovations, Inc.
FACE Supply Chain
Certified Conformant FACE Suppliers

FACE Portable Components Segment (PCS)
Collins Aerospace, Honeywell, L3Harris, Raytheon, Textron

FACE Transport Services Segment (TSS)
ADlink, Real-Time Innovations, Inc. (RTI)

FACE Operating Systems Segment (OSS)
DDC-I, DornerWorks, Green Hills, Wind River
FACE RTCA DO-178C Supply Chain
FACE Certified Conformant Suppliers with COTS DO-178C Certification Evidence

FACE Portable Components Segment (PCS)
Collins Aerospace, L3Harris, Raytheon

FACE Transport Services Segment (TSS)
Real-Time Innovations, Inc. (RTI)

FACE Operating Systems Segment (OSS)
DDC-I, Green Hills, Wind River
RTI Certification Partners

- AdaCore [Ada Solutions]
- Abaco [Boards]
- AFuzion [Training]
- Ansys [Design Tools]
- CoreAVI [Graphics Drivers]
- Curtiss-Wright [Boards]
- DDC-I [RTOS]
- Disti: [Graphics]
- Ensco: [Graphics]
- Green Hills Software [RTOS]
- Intel [Processors]
- LDRA [Test Tools]
- Lynx Software [RTOS]
- Mercury Systems [Boards]
- North Atlantic Industries [Boards]
- Rapita Systems [Test Tools]
- Presagis [Graphics]
- QNX [RTOS]
- Sysgo [RTOS]
- The Mathworks [Design Tools]
- Vector [Test Tools]
- Verocel [Cert Tools]
- Wind River [RTOS]
- WolfSSL [Security]
RTI Certification Partner Ecosystem Solution Stack

**Avionics Innovation**
- FAA RTCA DO-178C

**Avionics Innovation**
- FAA RTCA DO-178C

**RTI Connext DDS**
- FAA RTCA DO-178C

**RTI Connext DDS Databus**

- **DDC-I, GHS, Lynx, QNX, Wind**
  - Operating System / RTOS
  - FAA RTCA DO-178C

- **Abaco, CW, Mercury, NAII**
  - Board Vendors
  - FAA RTCA DO-254

- **ARM, Intel, NXP, TI, more**
  - Microprocessor
  - FAA RTCA DO-254

**RTI Certification Partners**
- FAA Safety Standards

**Real-Time Innovations**

©2021 Real-Time Innovations, Inc.
Varon Vehicles Skyscraper Project

Considerations
• Safety
• Security
• Regulatory
• Political
• Technical
• Financial
• Educational
• Operational
Questions?
Stay Connected

rti.com
Free trial of Connext DDS

@rti_software

rtisoftware

@rti_software

connextpodcast

@rti_software

rti.com/blog

Chip Downing
chip@rti.com
650-712-0655