Securing Multi-Domain Data-in-Motion in Complex Systems

Chip Downing

Senior Market Development Director,
Aerospace & Defense, RTI

Paul Tingey

Senior Field Application Engineer

Securing Multi-Domain Data-in-Motion in Complex Systems

Paul Tingey

Senior Field Application Engineer, EMEA, Real-Time Innovations, Inc.

The Demand for Data-Centricity

DoD Data Strategy

30 Sep 2020

Unleashing Data to Advance the National Defense Strategy

"It is the responsibility of all DoD leaders to treat data as a weapon system and manage, secure, and use data for operational effect"

Vision: "The DoD is a data-centric organization that uses data at speed and scale for operational advantage and increased efficiency"

7 Goals to Becoming a Data-Centric DoD

1. Make Data Visible -- Consumers can locate the needed data
2. Make Data Accessible -- Consumers can retrieve the data
3. Make Data Understandable -- Consumers can recognize the content, context, and applicability
4. Make Data Linked - Consumers can exploit data elements through innate relationships
5. Make Data Interoperable -- Consumers have a common representation / comprehension of data
6. Make Data Trustworthy -- Consumers can be confident in all aspects of data for decision-making
7. Make Data Secure -- Consumers know that data is protected from unauthorized use / manipulation

Multi-Domain Operations (MDO)

- The foundation of a Data-Centric DoD is Multi-Domain Operations (MDO)
- MDO describes how the U.S. Army, as part of the Joint Force consisting of the US Army, US Navy, US Air Force, and US Marines can counter and defeat a near-peer adversary capable of contesting the U.S. in all domains -- air, land, maritime, space, and cyberspace -- in both lethal and non-lethal competitions.
- MDO needs to integrate and assimilate data from all Armed Forces and from all contested domains to succeed.
- A Multi-Domain Battle enables the Joint Force to maneuver and achieve objectives, exploit opportunities, or create dilemmas for the enemy.
- Using Data the Joint Force can present multiple complementary threats where each threats requires a response, thereby exposing adversary vulnerabilities to other threats.

The Ultimate Goal of MDO is JADC2

Joint All Domain Command and Control (JADC2)

- The DoD's concept to connect sensors from the Joint Forces into a single system of systems, all working as one
- Reduces decision-making time from days to minutes to seconds
- Depending on the scenario, commanders can simply *plug and fight* whatever systems they deem necessary for their operation
- A monumental task without a common communications framework and extensible ontology (common data model) that needs to be owned by the DoD

Three Options for Securing Data-in-Motion

1. Trust the Pipe, Encrypt Nothing
2. Don’t Trust the Pipe, Encrypt Everything
3. Zero Trust Architecture – Trust Nothing, Protects Data for Different Security Requirements

Current Security Challenges

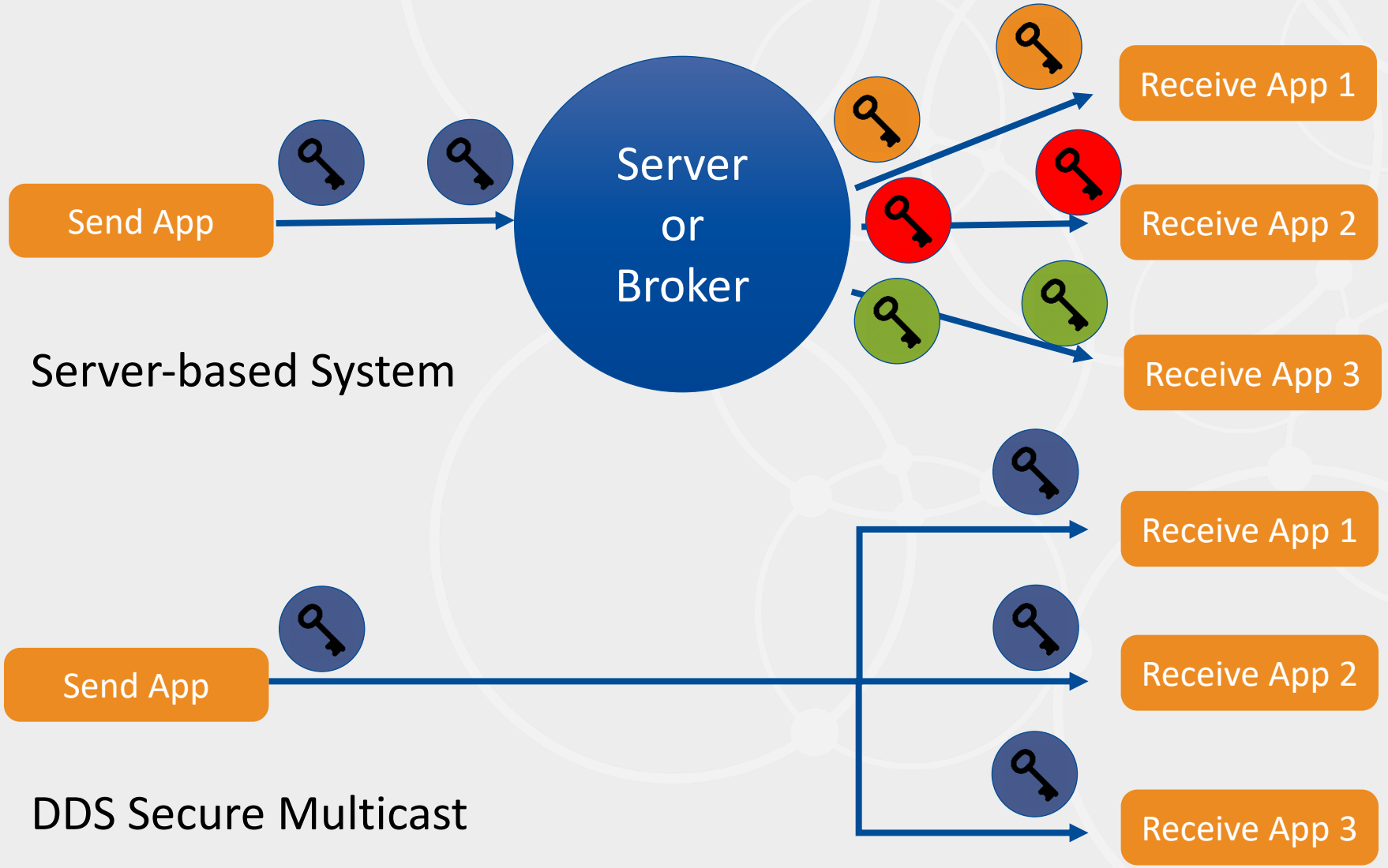
Current security is based on IT security

- Transport based (secure the pipe)
- Treats all the data the same
- Requires different channels for different security domains
- Poor support for MDO
- Vendor and platform specific
- Non-scalable

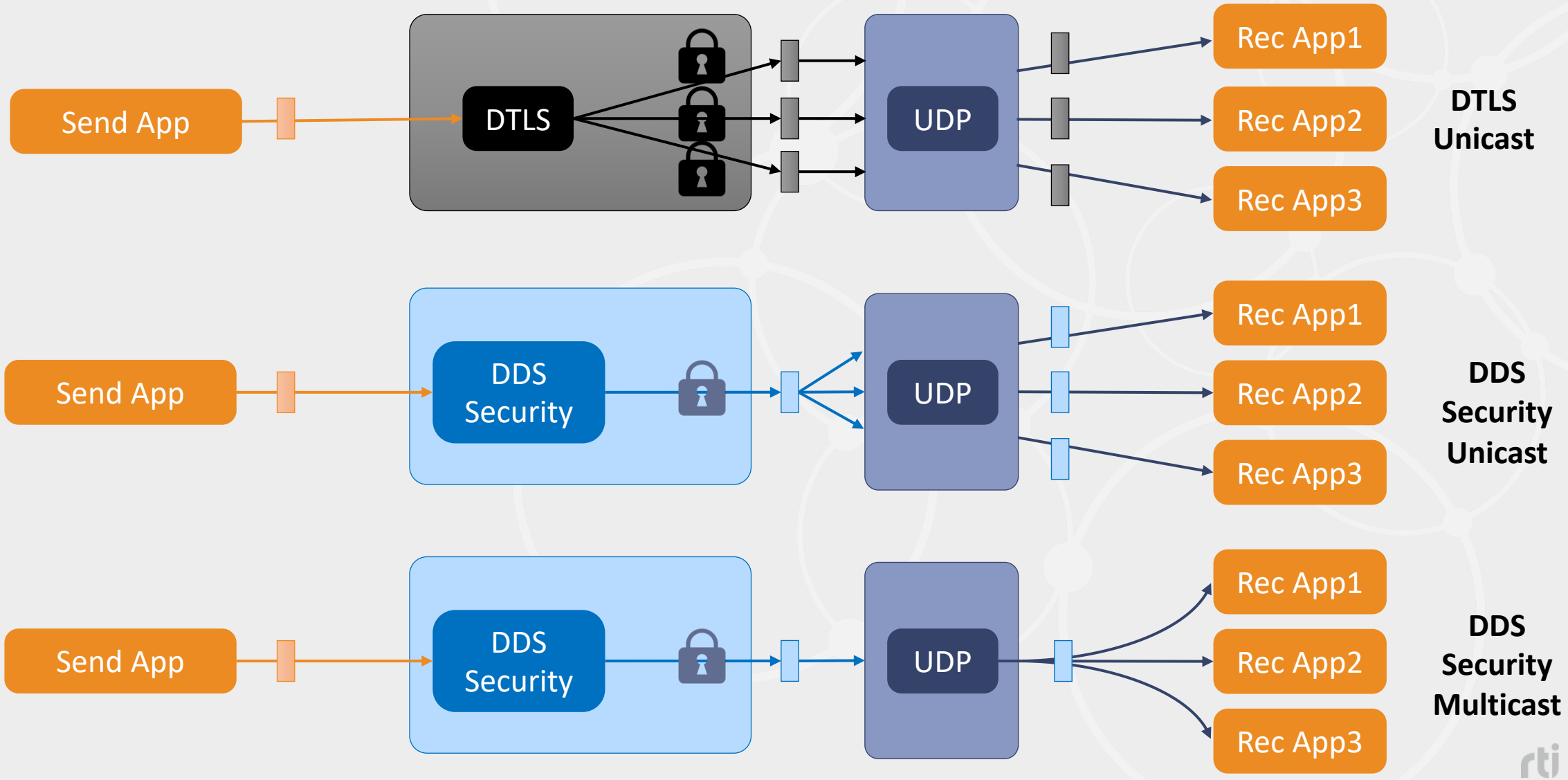
RTI DDS Secure, A New Approach to Security

- Secures data topics, not the pipe/machine/network
- Supports peer-to-peer authentication (no server or broker)
- Provides fine-grained security for each data topic
  - Controls what data is shared with specific coalition partners
- Massively parallel, scalable
  - Works for IT and OT platforms, simulation and deployed
- Supports MDO by design

Transport and Server Security vs DDS Security



Transport Security vs DDS Security

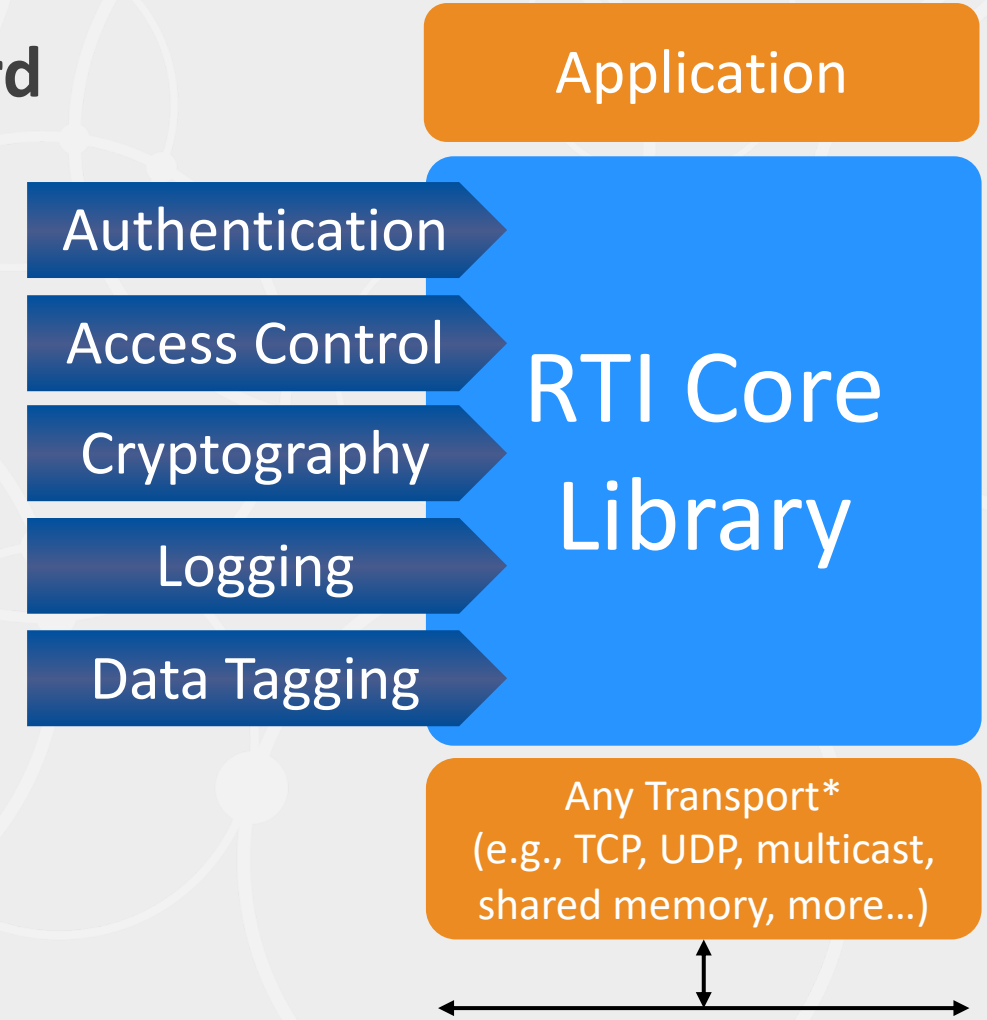


DDS Security Data-Centric Security Model

- Publishers are decoupled from subscribers
  - Enables a natural boundary for access control to information
- DDS can use standard PKI, cryptographic techniques, and other proven security components to enforce security policies
- Does not treat all data the same
  - Weather needs only to be authenticated to prevent spoofing
  - Tactical data would need full encryption

RTI Connext DDS Secure

- **Based on the OMG DDS Security Standard**
- **Built-in Plugins**
  - Little to no application development
- **Run over any transport**
  - TCP/UDP, serial, fiber, shared memory
- **Completely decentralized**
  - High performance and scalability
  - No single point of failure



Standard Capabilities with Security Plugins

Security Plugin	RTI Connext Secure Plugin Description
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

Data Components in a DDS Global Data Space

- **DDS Domain** -- The world of DDS data you are referencing
- **Topic** -- A group of related data elements
  - Similar to “type” or “schema”, with measured behavior (Quality of Service)
- **Instance** -- A unique element in the topic set of elements
  - Like the “key” fields in a database table
- **Databus** – An abstraction of data flows between publishers / subscribers

Logical

Physical

- **DDS Domain Participant** -- A connection to the Domain in order to source/observe observations
- **Data Writer** -- The source (publisher) of observations about a set of data elements (Topic)
- **Data Reader** -- Observer (consumer, subscriber) of a set of data elements (Topic)
- **Sample** -- An update of an instance (“message” or payload)

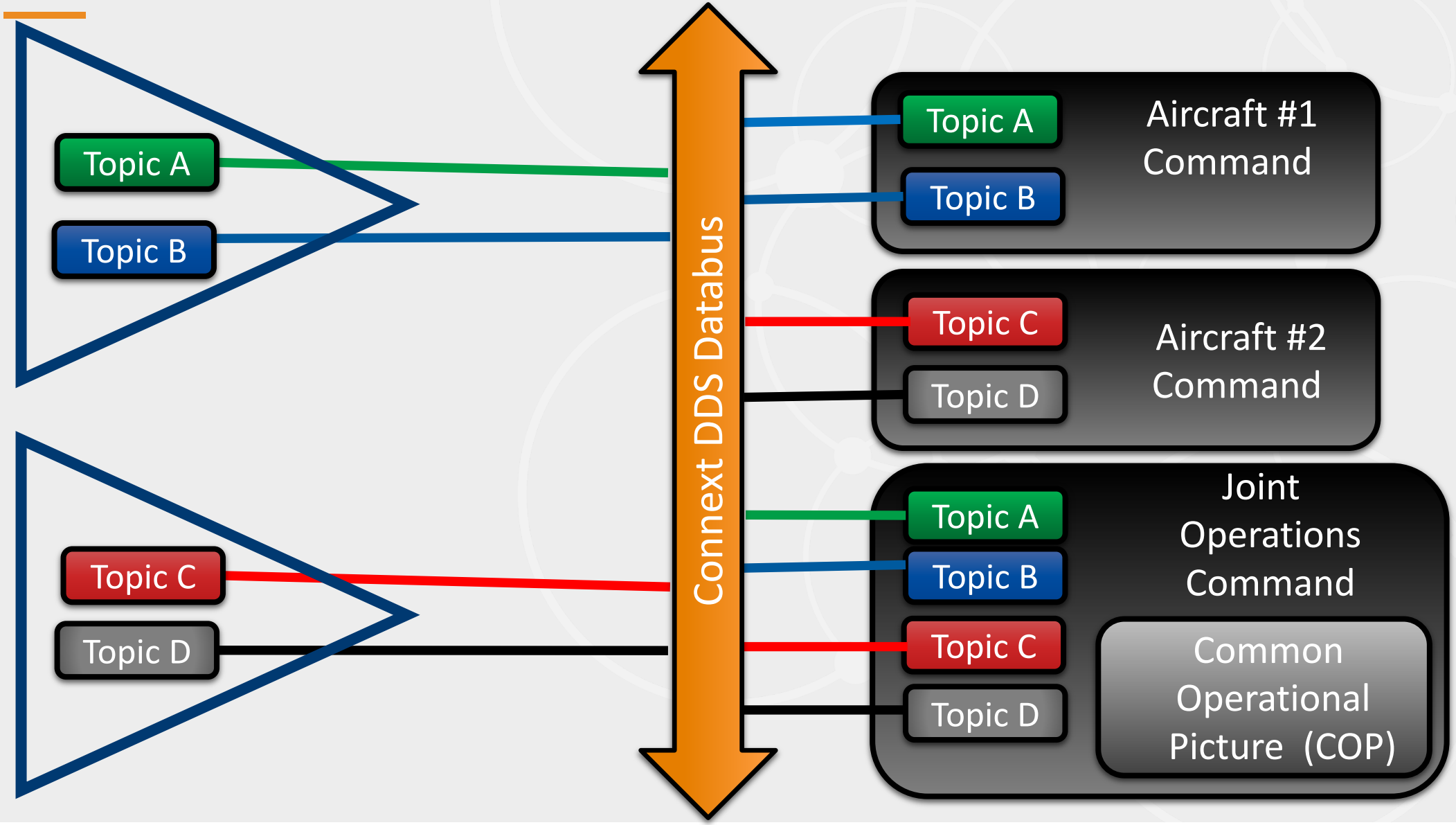
Security Domains

- **Security Domain** – A collection of data / IP made specifically available to an enclave of users and/or systems/networks
  - NIPRNet, SIPRNet, JWICS, NSANet, …
  - Army, Navy, Air Force, …
  - Google, Apple, Amazon, …
  - NATO, UK, US, …

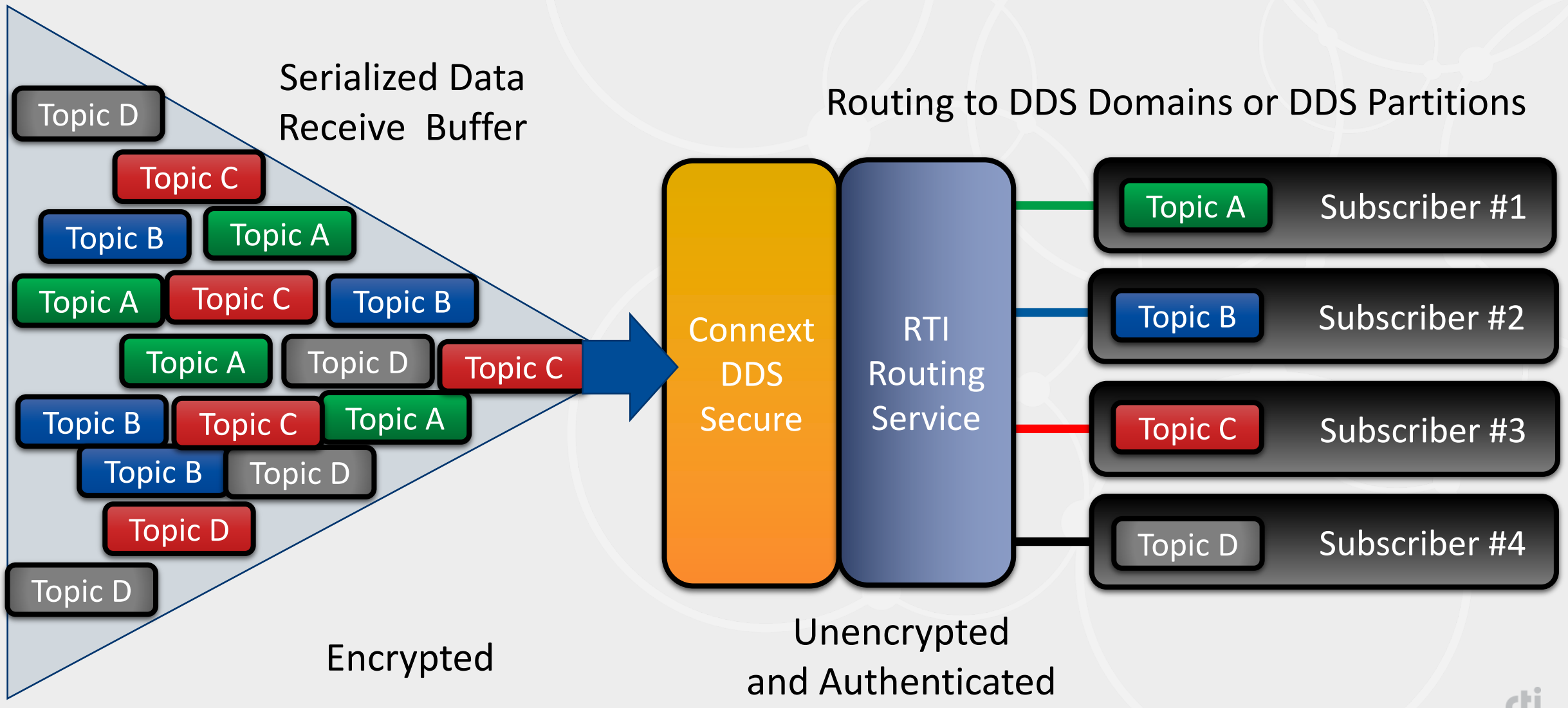
This is Data-in-Motion, not Data-at-Rest / Compute

- **This is not MILS – Multiple Independent Levels of Security**
  - A Separation Kernel (SK) managing compute partitions executing on a time and space basis on a shared compute platform
- **This is not MLS – Multiple Levels of Security**
  - A compute architecture that simultaneously manages multiple security domains
- **The is DDS Secure – Manages Data-in-Motion**
  - Individually secured topics on a network or a systems communications transport, not a compute container or compute partition

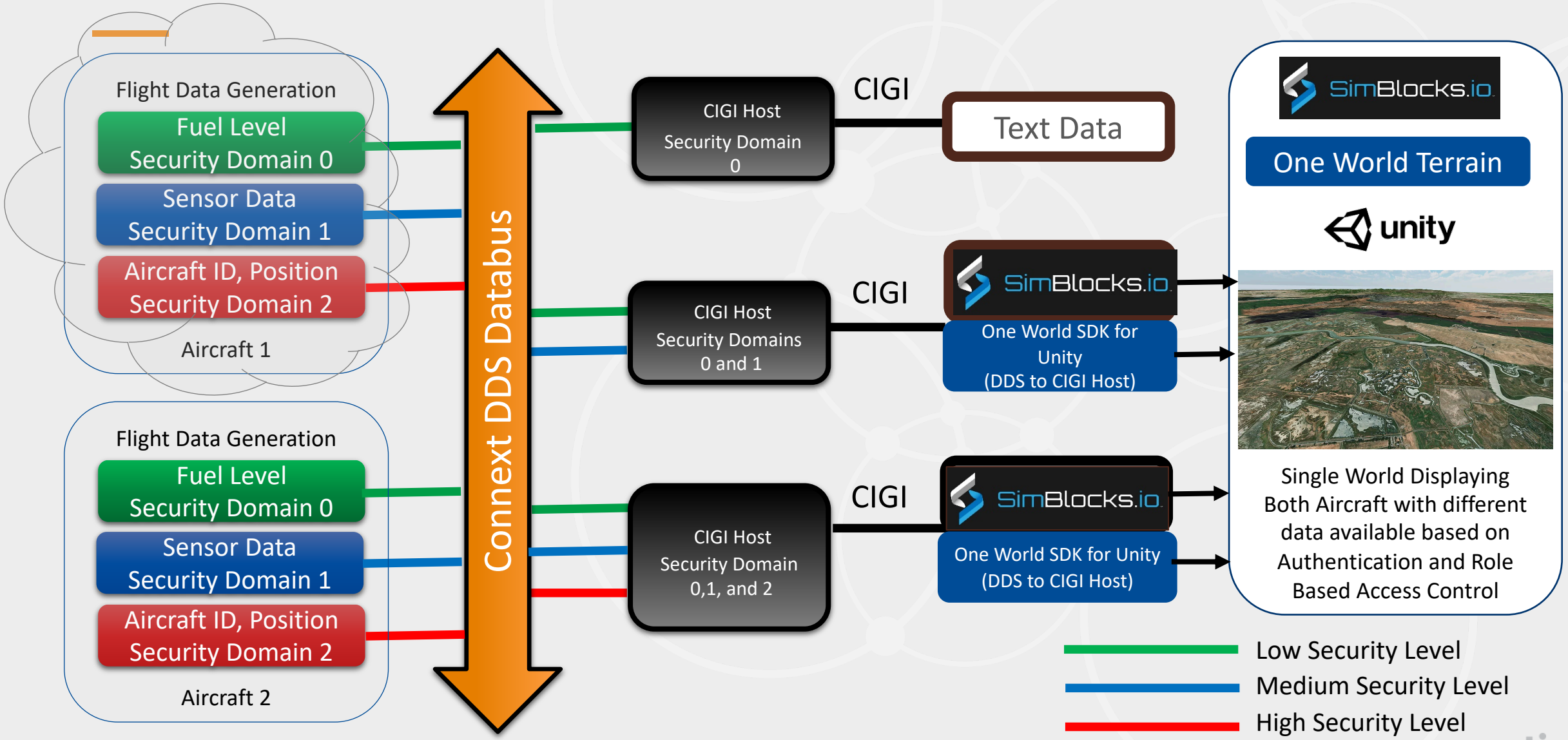
Connext DDS Secure Use Case – Joint Operations with COP



Connext DDS Routing Service – Security Topic Filter

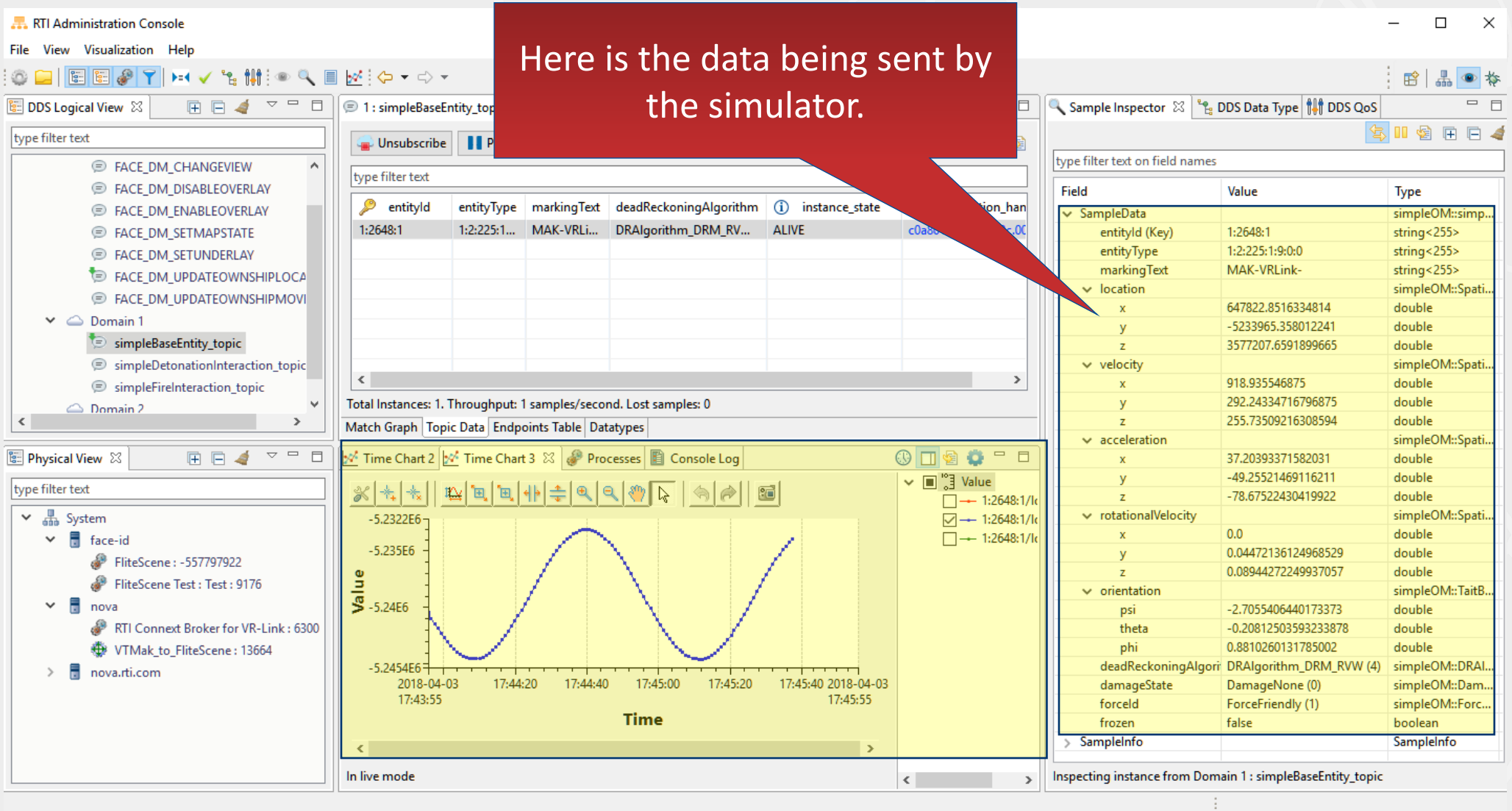


RTI Connext DDS Secure – 2 Simulated Aircraft

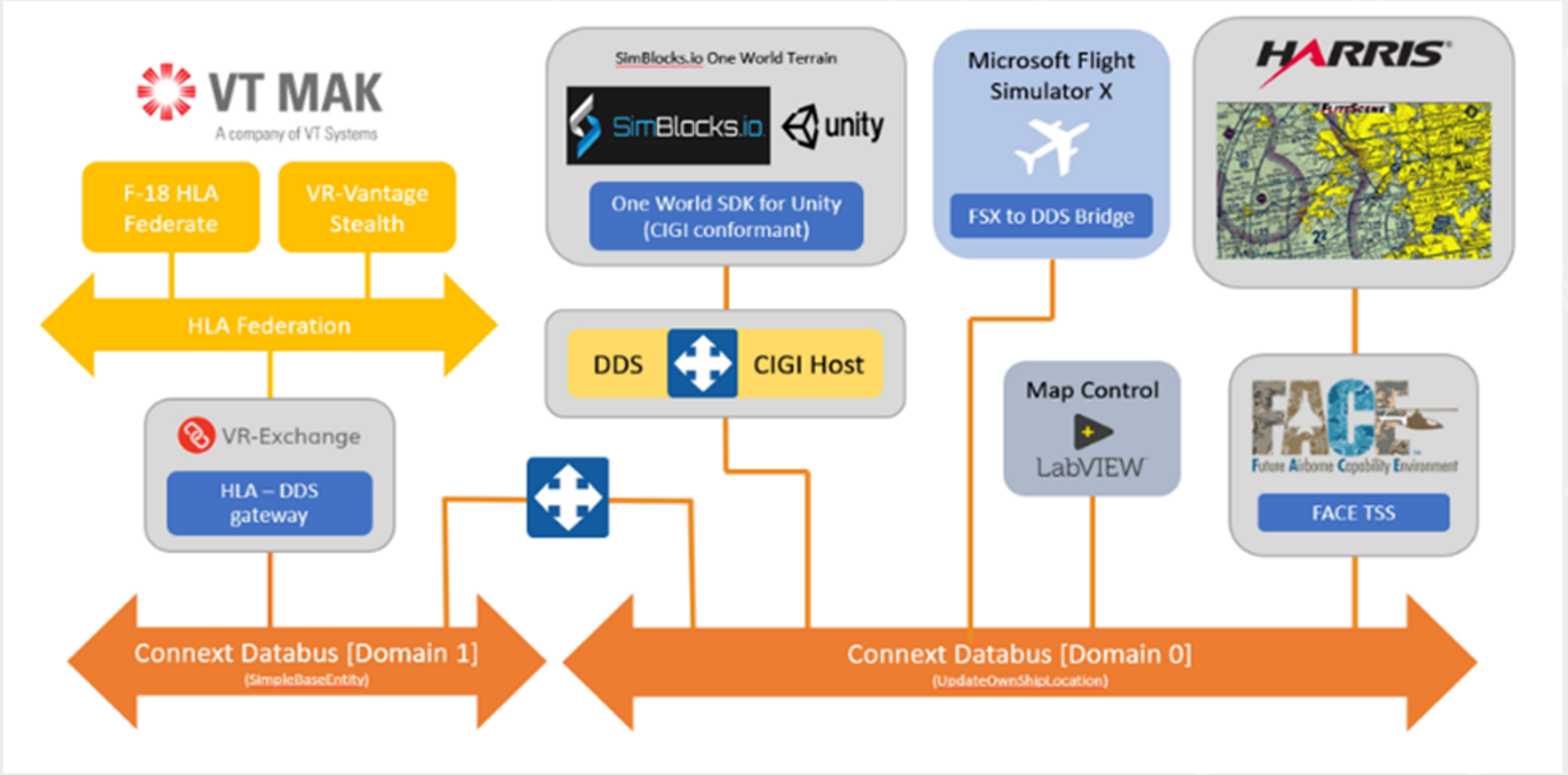


CIGI: wire data protocol standard that enables communications between an Image Generator and its host simulation platform

RTI Connext Admin Console



I/ITSEC Joint Demo



Mixed-Reality Multi Domain Operations with Connext DDS

Cloud

Management | Logging | Analytics | Other Services

Multi-Domain Operations (MDO) Global Connext DataBus

Secure Gateway

- Protocol/Data Interoperability
- Data Routing/Filtering

A Hierarchic, Loosely-Coupled Design Enables:

- Local Ownership
- Disconnected Operation
- Open Architecture
- Capability-as-a-Service
  - e.g., AI, Simulation, Data, Devices

Processing Location Agnostic / Transparent

Management | Logging | Analytics

Multi-Domain Operations (MDO) Cross-System Connext DataBus (Local/Regional)

DDS

One World Terrain

DataBus Gateway

AI Training Scenarios

Protocol Gateway

Protocol XYZ

Simulated Worlds

Sim@ NATO 2

Sim@ NATO 1

Sim@ SOCOM

OtherSim

Local Mgmt

Simulation Connext DataBus

Unity

Unreal

Simulated Actors

Digital Twins

Real World

Autonomous Systems

Air | Helo | Maritime | Ground

AI/ML/DL Augmented Reality

Real World Twin

Edge

Summary

- Data-Centricity enables operational dominance and survivorship
- RTI Connext DDS is data-centric by design
  - And is an open standard supporting MOSA directives
- RTI Connext DDS Secure efficiently enables trust and confidence in real-time data
- RTI Connext DDS and RTI Connext DDS Secure is the foundation of our next generation MDO Data-Centric DoD and JADC2

Questions?

Stay Connected

rti.com
Free trial of Connext DDS

rtisoftware

@rti_software

connextpodcast

@rti_software

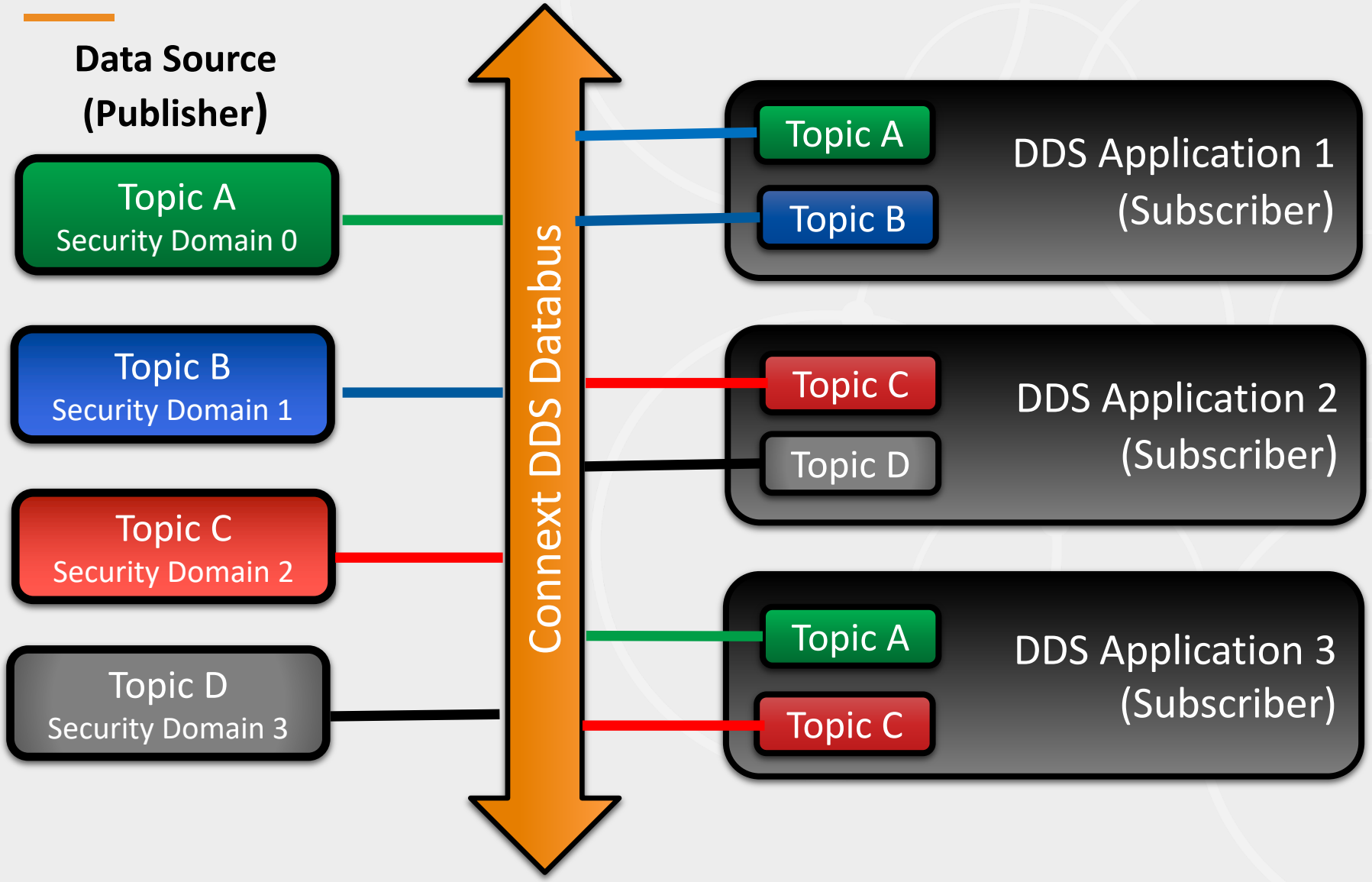
rti.com/blog

Try a full version of Connext DDS for 30 days

TRY CONNEXT AT
RTI.COM/DOWNLOADS

Includes resources to get you up and running fast

Connext DDS Secure -- Data-Centric Security



Simulation and Gaming Partners