Your systems.
Working as one.

Building Scalable Security for Systems of Systems

Paul Tingey
Senior Field Application Engineer

Index

- Building Scalable Distributed Systems
  - Introduction to IIoT Framework Solutions
  - DDS Principles
- Securing the Data on Distributed Systems
- Fine-Grain DDS Security
- Conclusion

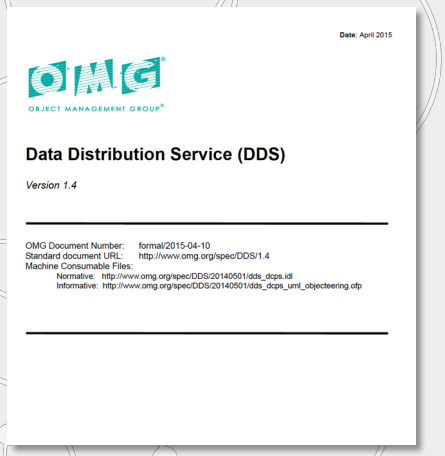
RTI in the Industrial IoT

- RTI is the largest embedded middleware vendor
- 1000+ designs, many real-world programs across industries
- Full DDS, tools, services, support, secure and certified versions
- About 200 people

An Overview of Data Distribution Service (DDS)

OMG Data Distribution Service

- First version of the DDS standard was released in 2004
- Most recent version (v1.4) was released in April 2015
- "Data-Centric Publish-Subscribe model for distributed application communication and integration"


Date: April 2015

OBJECT MANAGEMENT GROUP

Data Distribution Service (DDS)

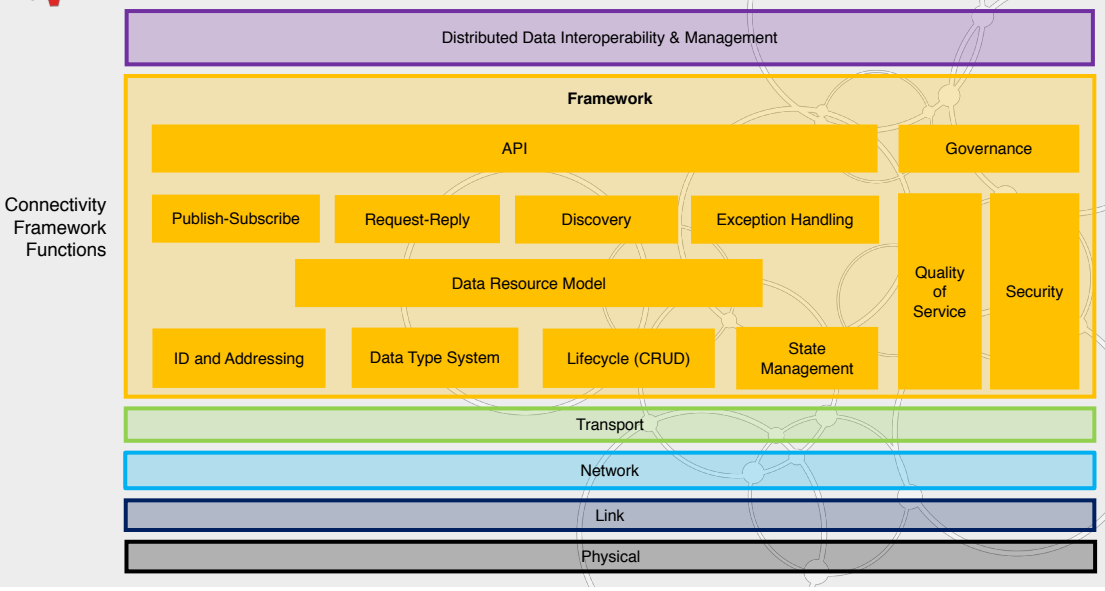
Version 1.4

OMG Document Number: formal/2015-04-10
Standard document URL: http://www.omg.org/spec/DDS/1.4
Machine Consumable Files:
Normative: http://www.omg.org/spec/DDS/20140501/dds_dcps.idl
Informative: http://www.omg.org/spec/DDS/20140501/dds_dcps_uml_objecteering.ofp

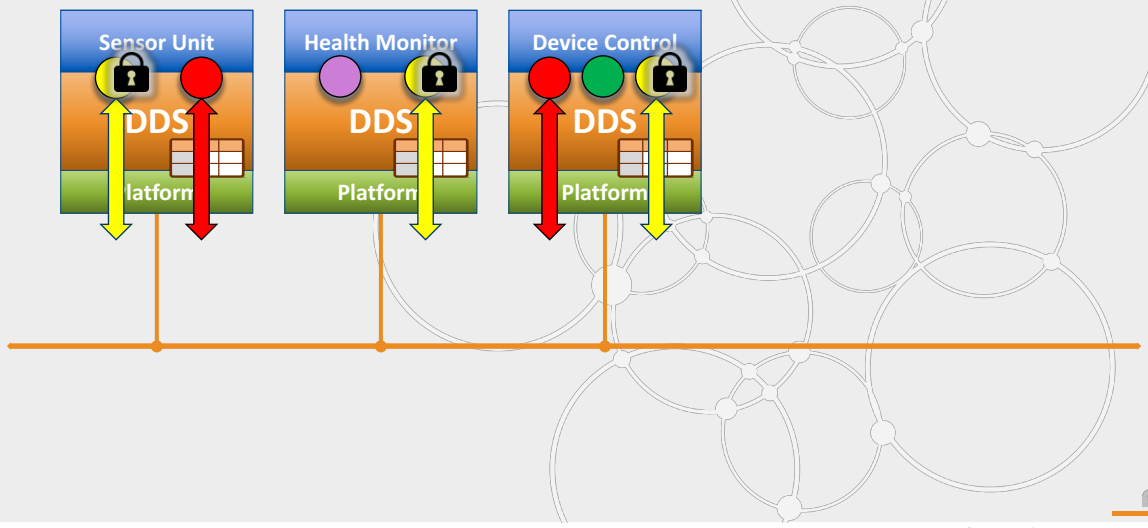
What is the Data Distribution Service… ?

- DDS is ideally suited to applications that are required to share large amounts of data in a fast, secure, scalable and reliable way
- It was originally designed for mission critical systems and is now at the heart of many *Open Architecture* initiatives in A&D
- It's *TRL-9* technology used widely in the "L" parts of *LVC* systems
- It's widespread use in military systems has led to strong interest in the simulation and training market
- DDS is Publish-Subscribe, Data-Centric and Peer-to-Peer
  - enabling location transparency, decentralized operation, dynamic scalability and real-time performance

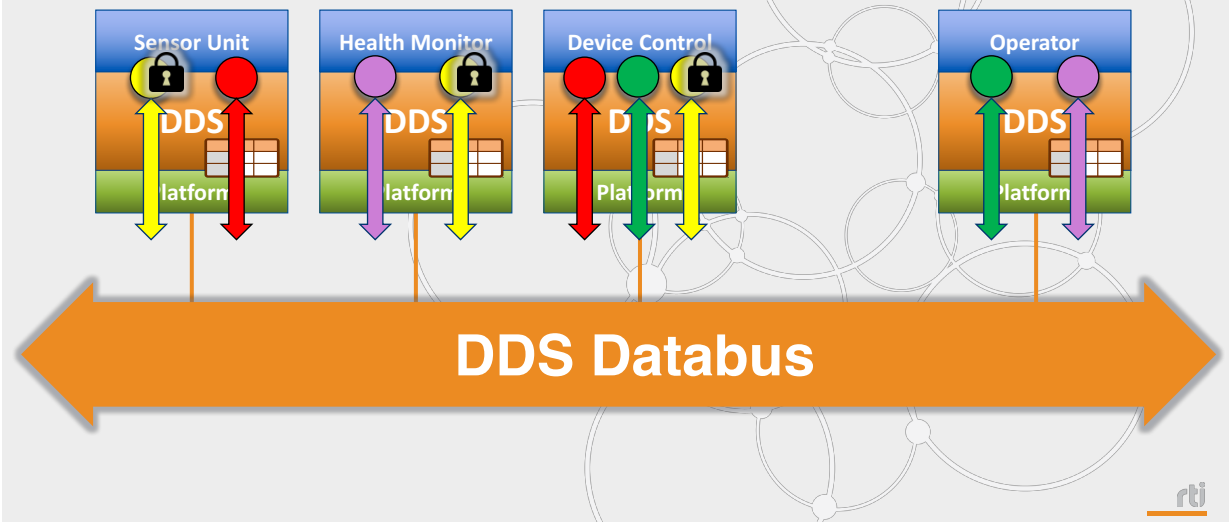
Connectivity Framework Layer



Connection via the DDS Databus…



Connection via the DDS Databus…



Connection via the DDS Databus…

A Data Model (written in IDL) describes the data in the system and allows DDS to 'understand' and manage data in the system appropriately.

DDS provides an API to the programmer (which RTI wrap in language bindings) to enable data-centric access to your data.

Data flows are configured via Quality of Service settings that define how data is delivered between nodes in the distributed system. In DDS terminology these data flows are called Topics.

DDS abstracts the application away from the Operating System making the application less complex, more portable and transport agnostic.

Data is cached at the endpoints by DDS (based on the QoS settings); the application always has the data it requires when it requires it.

DDS operates peer-to-peer to give real-time performance and meaning there is no central server.

DDS optimises network usage by filtering data appropriately (at either source or destination) and only delivering data when and where it is needed.

About Data Centricity

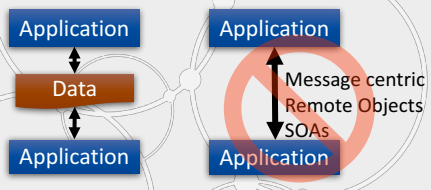
Data Centricity Definition

a) The interface *is* the data.
b) The infrastructure understands that data.
c) The system manages the data and imposes rules on how applications exchange data.

Database

Data centric storage and searching of old data

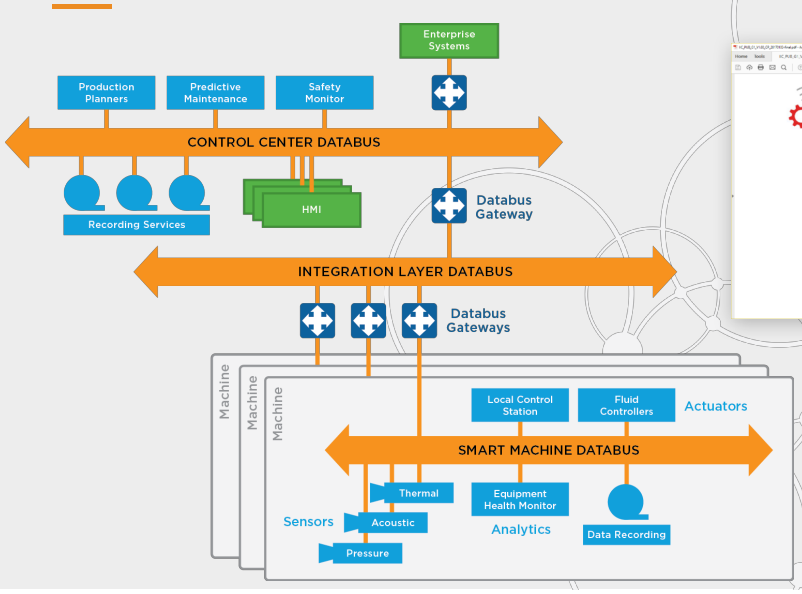
```
SELECT * FROM ShapeData
  WHERE color='RED' AND shapesize > 10;
```

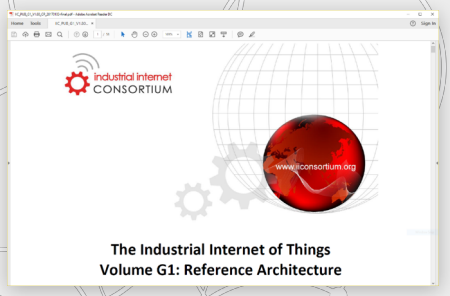


Data centric sharing and filtering of future data

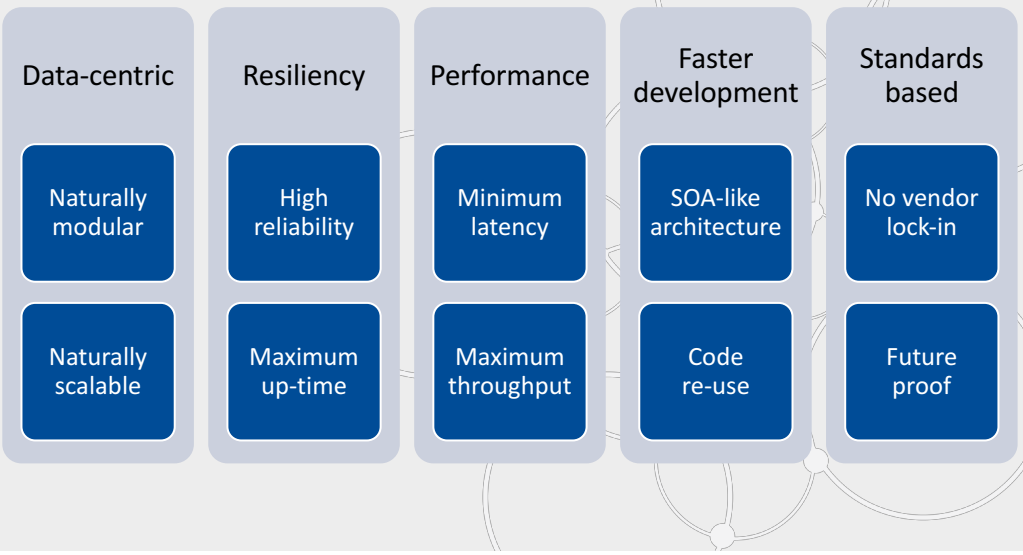
```
cft = create_contentfilteredtopic_with_filter(
  "MyFiltered_topic", ShapeData_topic,
  "(color MATCH 'RED') AND (shapesize > 10)", … );
```


The IIC Layered Databus Architecture Pattern





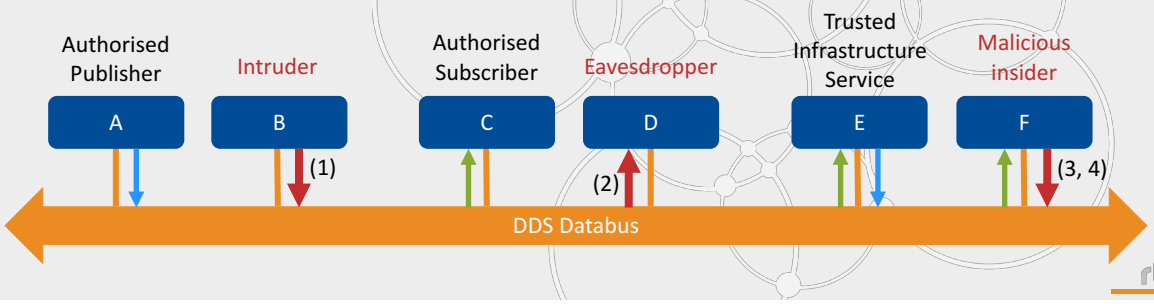
Why DDS ?



Securing the Data on Distributed Systems

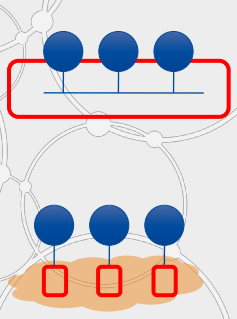
Associated Threats

- For DDS based (distributed) systems, the four most relevant threat categories are:
  1. Unauthorised publication
  2. Unauthorised subscription
  3. Tampering and replay
  4. Unauthorised access to data by infrastructure services



Approaches to Protect DDS

- Transport Layer Security
- Fine-Grained Data Security



Transport-Level Secure Data Transfer

- Can use TLS or DTLS
- Method involves:
  1. Authenticate
     - Verify your identity
  2. Securely exchange cryptographic keys
  3. Use keys to:
     - Encrypt data
     - Add a message authentication code

Limitations of Transport-Level Security

- Can be inefficient: all data is encrypted and signed
  - Application data and metadata
  - Regardless of whether confidentiality and/or integrity are required
- Poor latency and jitter: usually runs over TCP
- Not scalable: no multicast support
  - Even with DTLS over UDP
- Apps are authenticated or they're not
- No inherent protection against insider threats
  - E.g.: authorized subscriber but unauthorized publisher
- Access control has to be done at application level

Fine grained DDS Security

OMG DDS Security Standard

- OMG released the DDS Security specification (v1.1) in July 2018
- Collaboratively developed by a number of DDS vendors
- Defines:
  - DDS Security Model
  - Service Plugin Interface (SPI) Architecture


An OMG® DDS Security™ Publication

OBJECT MANAGEMENT GROUP®

DDS Security

Version 1.1

OMG Document Number: formal/2018-04-01

Release Date: July 2018

Standard Document URL: https://www.omg.org/spec/DDS-SECURITY/1.1

Machine Consumable Files:

Normative:

https://www.omg.org/spec/DDS-SECURITY/20170901/dds_security_plugins_spis.idl
https://www.omg.org/spec/DDS-SECURITY/20170901/omg_shared_ca_governance.xsd
https://www.omg.org/spec/DDS-SECURITY/20170901/omg_shared_ca_permissions.xsd
https://www.omg.org/spec/DDS-SECURITY/20170901/dds_security_plugins_model.xmi

Non-normative:

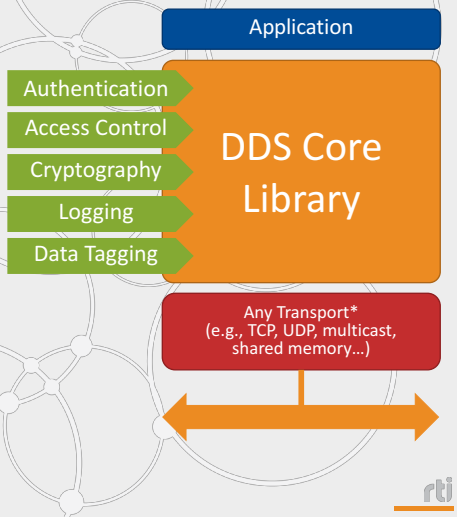
https://www.omg.org/spec/DDS-SECURITY/20170901/omg_shared_ca_governance_example.xml
https://www.omg.org/spec/DDS-SECURITY/20170901/omg_shared_ca_permissions_example.xml

OBJECT MANAGEMENT GROUP

DDS™

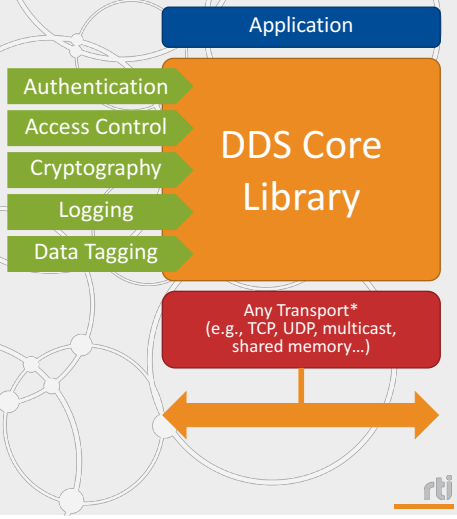
OMG DDS Security Standard

- Based on OMG DDS Security spec
- Built-In Plugins
  - Little to no change required to DDS applications
  - Security is configured through XML
- Optional SDK available to customize plugin behavior
- Runs over any transport
  - Does not require TCP or IP
  - Secure Multicast for scalability, low latency
- Completely decentralized
  - High performance and scalability
  - No single point-of-failure



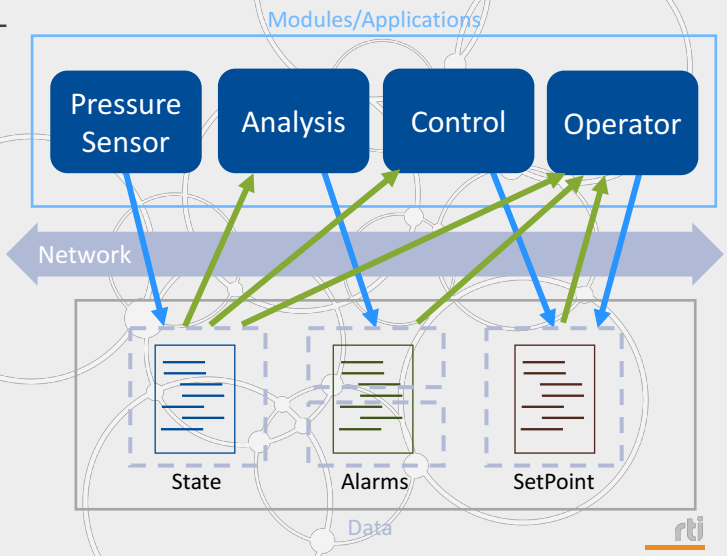
OMG DDS Security Standard

- The Service Plugin Interface (SPI) Architecture defines interfaces for five plugins
  - Authentication
    - Verification of the identity of an application
  - Access Control
    - Allows enforcement of policies (e.g. write access to a topic)
  - Cryptography
    - An interface to crytographic functionality
  - Logging
    - Auditing of DDS Security related events
  - Data Tagging
    - Enables adding tags to data samples



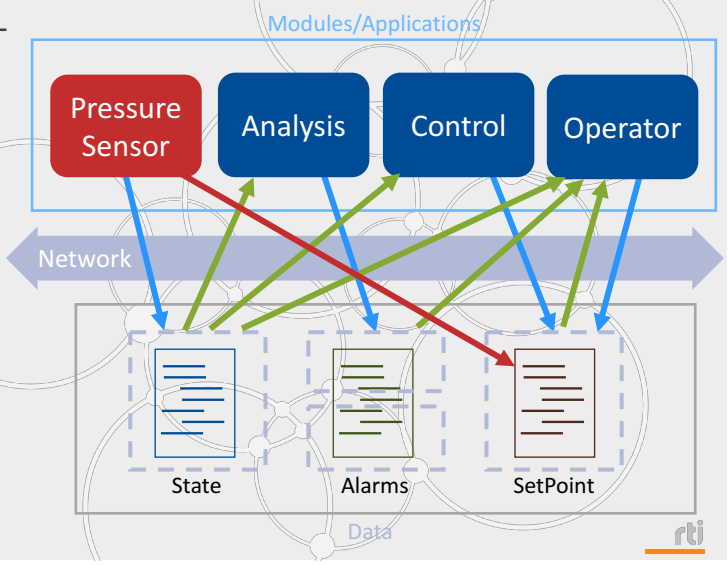
Fine-Grained Data-Centric Security

- DDS Security provides fine-grained security in distributed systems
- Enables the securing of individual data flows (topics)
- In the system shown here the SetPoint data item should be secured
  - Transport level security (TLS) provides only partial protection



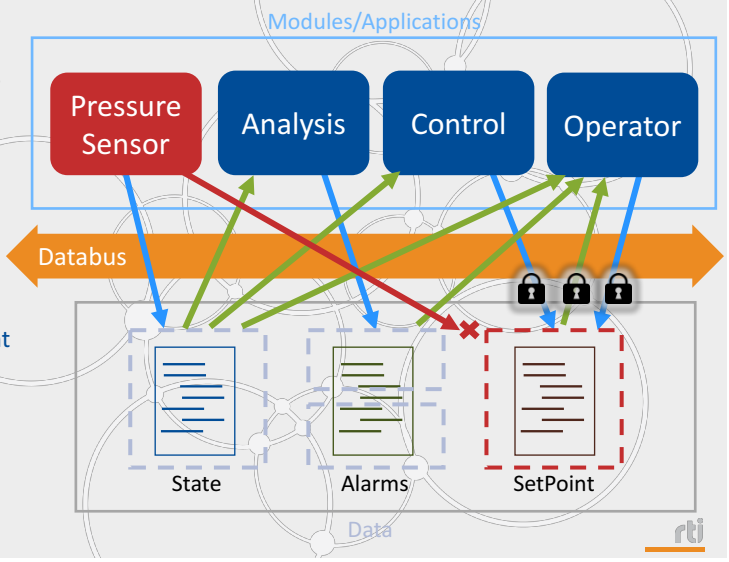
Fine-Grained Data-Centric Security

- DDS Security provides fine-grained security in distributed systems
- Enables the securing of individual data flows (topics)
- In the system shown here the SetPoint data item should be secured
  - Transport level security (TLS) provides only partial protection



Fine-Grained Data-Centric Security

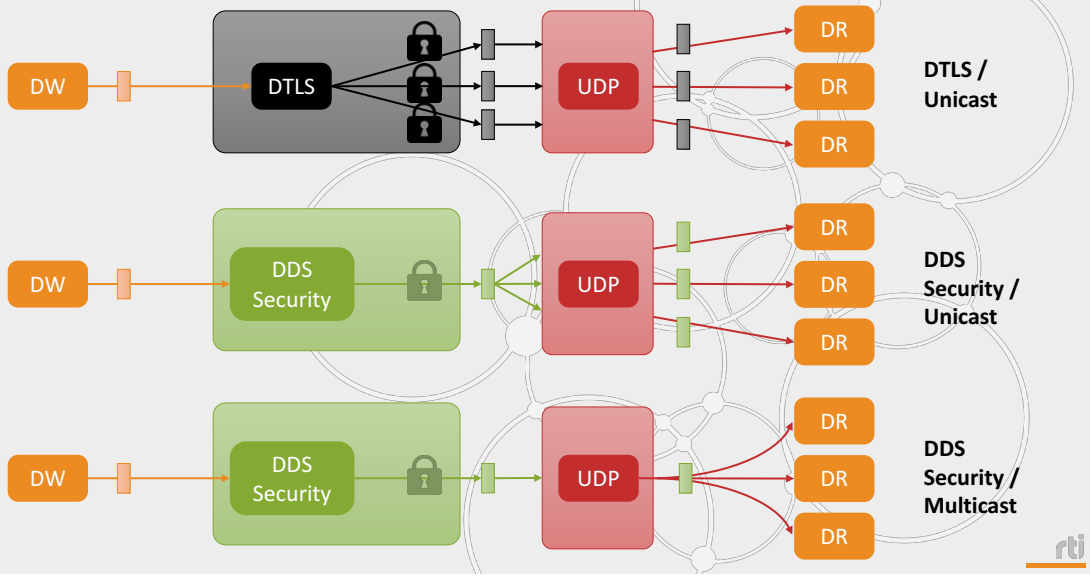
- DDS Security enables fine grained security of a Topic
  - For example, for SetPoint, for Authentication and Access Control
- Only specific modules/apps will then be able to access the Topic, e.g.
  - Operator can publish SetPoint
  - Operator can subscribe to Setpoint
  - Control can publish Setpoint
- Modules/apps without the correct security settings will not have access



Fine Grained Control to Optimize Performance

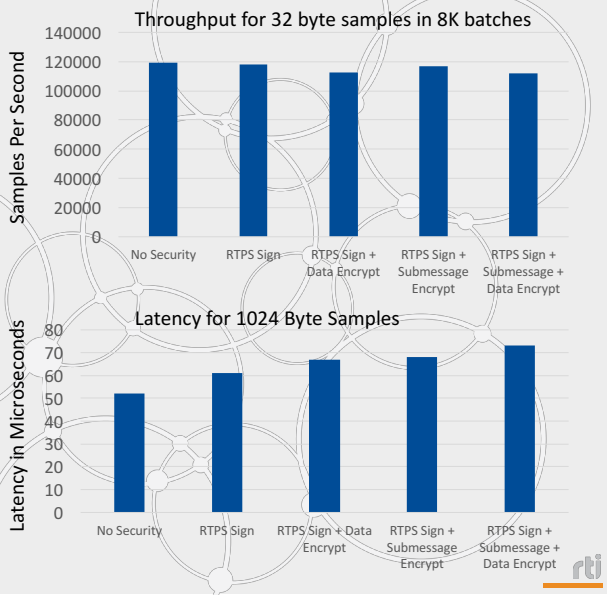
- DDS Security allows very fine grained control of security
  - Choose from:
    - Unsecured (data sent in the clear without a signature)
    - Signed with a Galois Message Authentication Code (GMAC) for integrity
    - Encrypted and signed
  - Configurable per:
    - Domain for metadata (discovery, liveliness)
    - Topic (whole RTPS message or user data only)

Transport Security vs DDS Security



Performance

- DDS Security provides an environment for high performance security through:
  - Fine-grained security selections that match your requirements
  - A pluggable architecture to allow use of your own customised algorithms (h/w or s/w)
  - Support for security over multicast



Conclusions

- DDS is a mature standard from OMG
  - Focuses on efficient data-distribution for real-time and high-performance systems
  - Mandated and Deployed worldwide in Military systems and other demanding real-time applications
  - Platform neutral, with a Portable API and Interoperable Wire Protocol
  - Highly Tunable via Quality of Service (QoS)
- DDS is extended with a OMG managed specification for Security
  - Granular data security
  - Pluggable architecture for customized protocols
  - Runs over any transport
  - Optimises network usage with support for security over multicast

Thank You