RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: LAB3-W13

Securing The Industrial IoT: A Deep Dive into the Future

Hamed Soroush, Ph.D
Senior Research Security Engineer
Real-Time Innovations (RTI)
@HamedSoroush

Gerardo Pardo, Ph.D
Chief Technology Officer
Real-Time Innovations (RTI)

Rose Wahlin
Principal Software Engineer
Real-Time Innovations (RTI)
@ProjectDerby

#RSAC

Outline

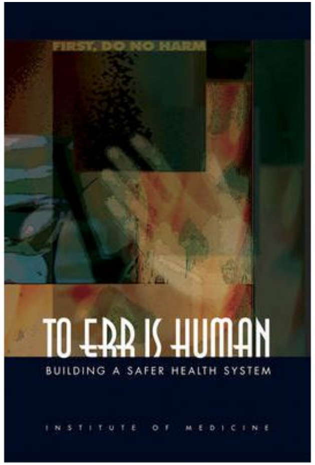
- Medical IoT: Need for More Safety & Security
  - Hacking Integrated Clinical Environments: A Demo
  - Need for granular security
- Introduction to Data Distribution Service (DDS)
- DDS Security: Design, Rationale, Hands-On Exercises
- Concluding Remarks

Medical IoT: Opportunities & Challenges

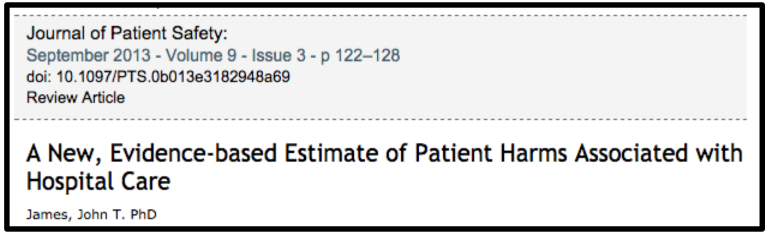
Need for Improved System Integration, Device Interoperability, and Granular Security

What Is Wrong In This Picture?

What is Wrong With These Stats?



1999: 98000 deaths per year due to mistakes in hospitals

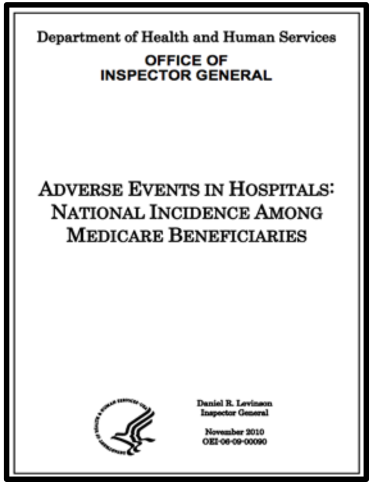


Journal of Patient Safety:
September 2013 - Volume 9 - Issue 3 - p 122–128
doi: 10.1097/PTS.0b013e3182948a69
Review Article

A New, Evidence-based Estimate of Patient Harms Associated with Hospital Care

James, John T. PhD

2013: 210,000-440,000 hospital patients suffer from preventable harm contributing to their death, making it the third leading cause of death after heart disease and cancer



Department of Health and Human Services
OFFICE OF
INSPECTOR GENERAL

ADVERSE EVENTS IN HOSPITALS:
NATIONAL INCIDENCE AMONG
MEDICARE BENEFICIARIES

Daniel R. Levinson
Inspector General

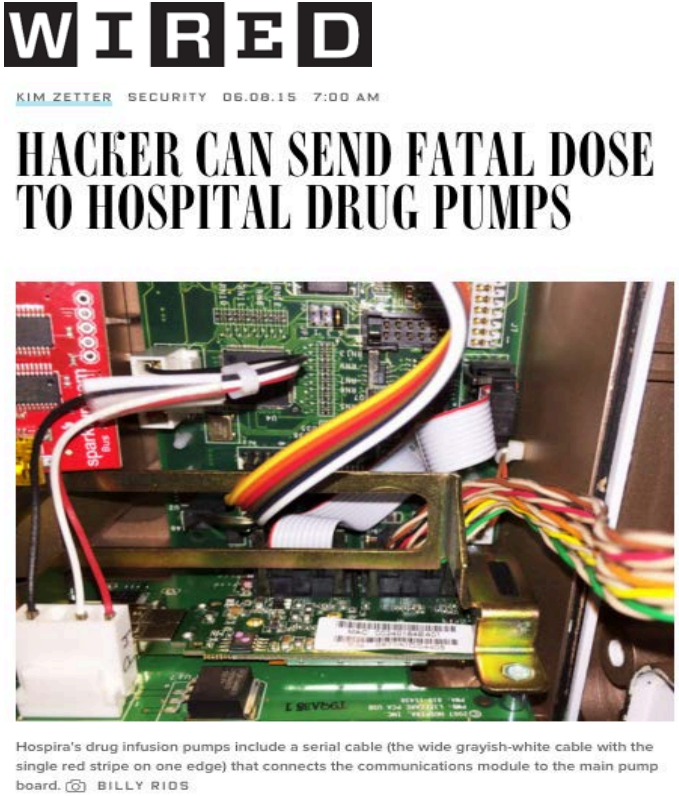
November 2010
OEI-06-09-00090

2010: Bad hospital care contributed to 180,000 patient deaths in Medicare alone

PCA Safety: Current State

Current State of Patient Controlled Analgesia

And It Gets Worse…



WIRED

KIM ZETTER SECURITY 06.08.15 7:00 AM

HACKER CAN SEND FATAL DOSE TO HOSPITAL DRUG PUMPS

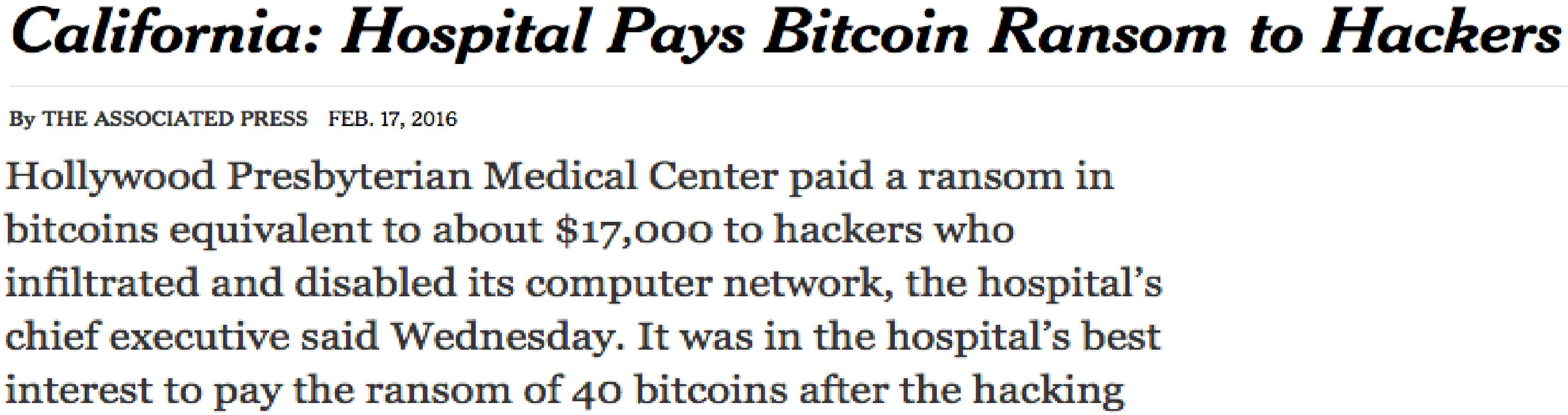
Hospira's drug infusion pumps include a serial cable (the wide grayish-white cable with the single red stripe on one edge) that connects the communications module to the main pump board. BILLY RIOS

A hacker could change the dosages of drugs delivered to patients and alter the pump's display screens to indicate a safe dosage was being delivered.

An attacker wouldn't need physical access to the pump because the communication modules are connected to hospital networks, which are in turn connected to the Internet.

And Worse…

The New York Times



California: Hospital Pays Bitcoin Ransom to Hackers

By THE ASSOCIATED PRESS FEB. 17, 2016

Hollywood Presbyterian Medical Center paid a ransom in bitcoins equivalent to about $17,000 to hackers who infiltrated and disabled its computer network, the hospital’s chief executive said Wednesday. It was in the hospital’s best interest to pay the ransom of 40 bitcoins after the hacking

Medical IoT Will Change All This

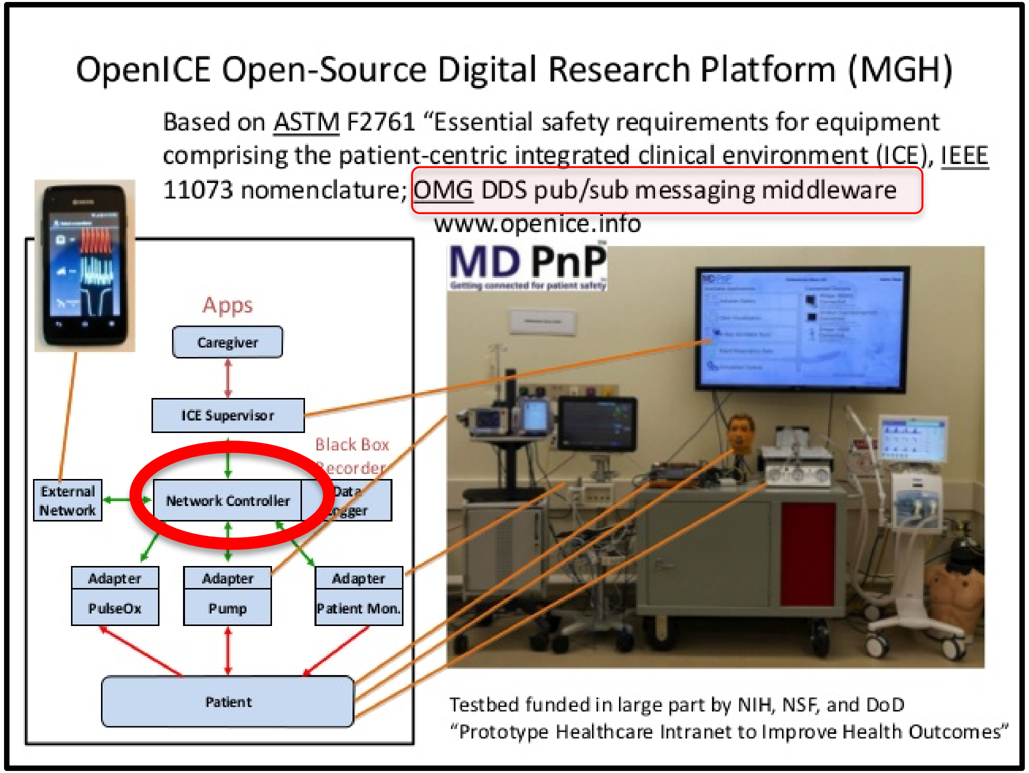
Hopefully…

Integrated Clinical Environment (ICE)

Automatic Discovery

Fully Peer-to-Peer Multicast Support

QoS Control:
e.g. Timing, Reliability,
Ownership,
Redundancy, Filtering,
Granular Security



OpenICE Open-Source Digital Research Platform (MGH)

Based on ASTM F2761 "Essential safety requirements for equipment comprising the patient-centric integrated clinical environment (ICE), IEEE 11073 nomenclature; OMG DDS pub/sub messaging middleware

www.openice.info

Testbed funded in large part by NIH, NSF, and DoD
"Prototype Healthcare Intranet to Improve Health Outcomes"

Protecting Communications

- Protecting ICE Communications at Transport Level
  - TLS or DTLS
  - Not sufficient in many cases due to lack of granular security

- Fine-grained Security for ICE (and other IoT Systems)

These approaches will be covered in more detail later in this talk

Why Fine Grained Security?

A Demo

RSAConference2016

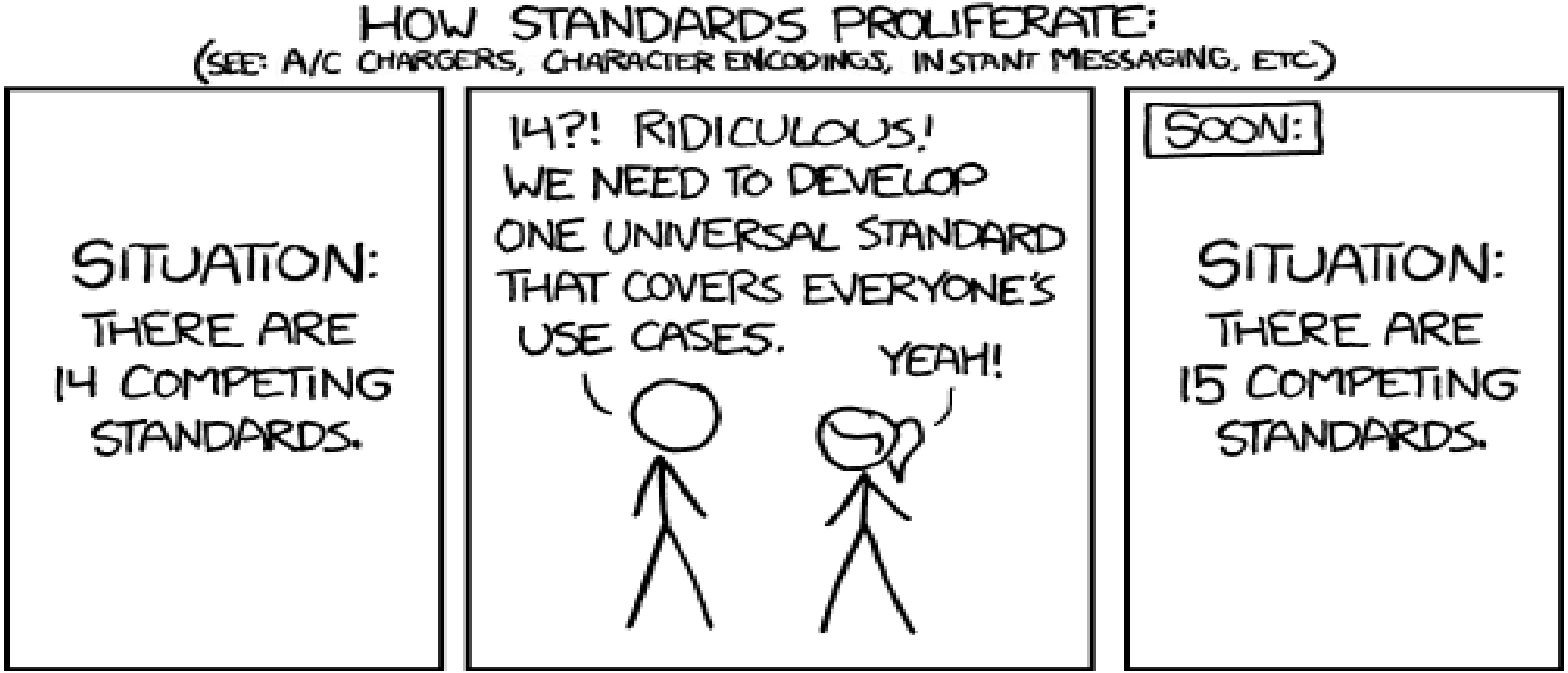
#RSAC

Introduction To Data Distribution Service

Gerardo Pardo, Ph.D

Chief Technology Officer

Real-Time Innovations (RTI)


HOW STANDARDS PROLIFERATE:
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC)
SITUATION: THERE ARE 14 COMPETING STANDARDS.
14?! RIDICULOUS! WE NEED TO DEVELOP ONE UNIVERSAL STANDARD THAT COVERS EVERYONE'S USE CASES.
YEAH!
SOON:
SITUATION: THERE ARE 15 COMPETING STANDARDS.

Industrial IoT Key System Characteristics

Large scale, heterogeneous, built with multi-vendor components, often broadly distributed and evolving

- Reliability
- Scalability
- Safety
- Security
- Resiliency

Industrial vs. Consumer IoT

Moore’s Insight Report, 2014

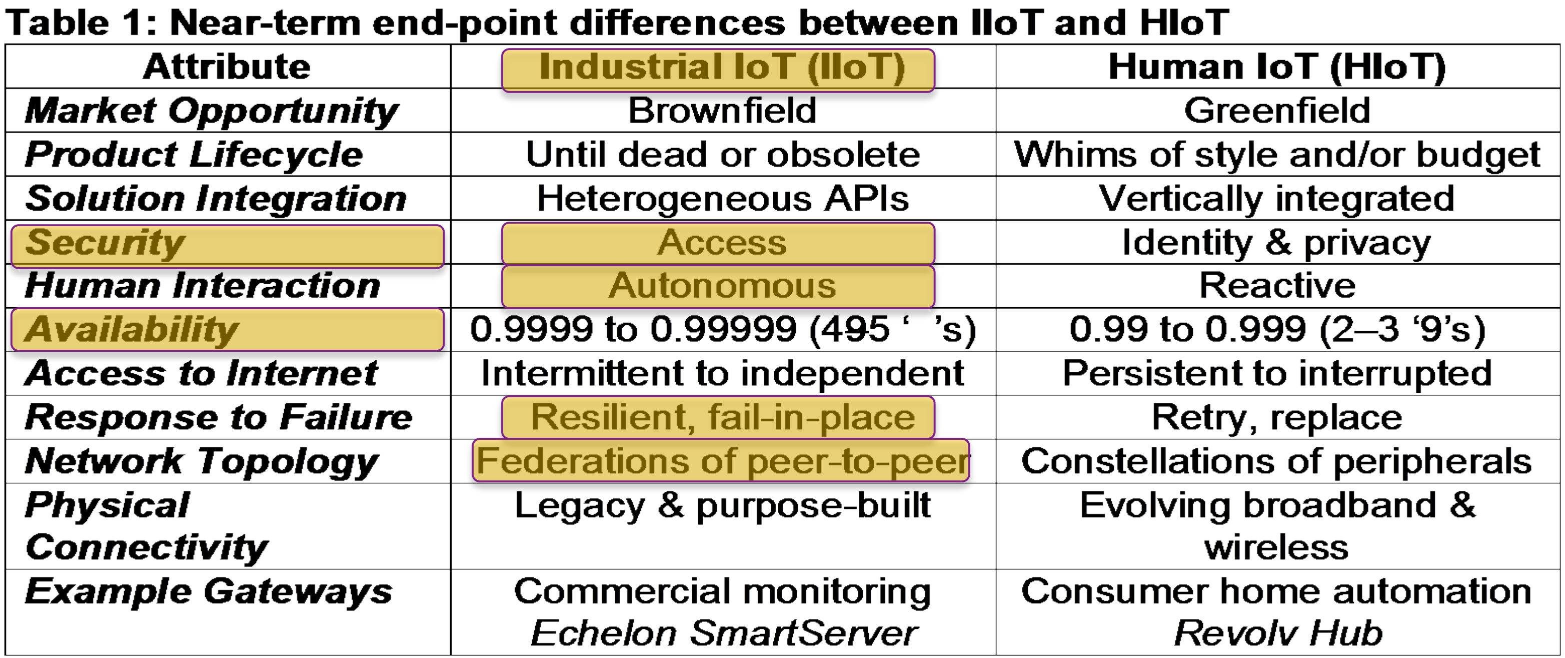


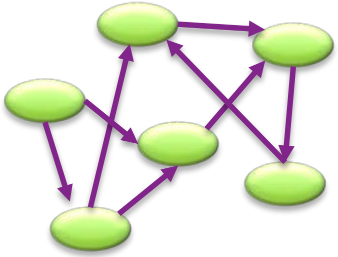
Table 1: Near-term end-point differences between IIoT and HIoT

Attribute	Industrial IoT (IIoT)	Human IoT (HIoT)
Market Opportunity	Brownfield	Greenfield
Product Lifecycle	Until dead or obsolete	Whims of style and/or budget
Solution Integration	Heterogeneous APIs	Vertically integrated
Security	Access	Identity & privacy
Human Interaction	Autonomous	Reactive
Availability	0.9999 to 0.99999 (495 ‘ ’s)	0.99 to 0.999 (2–3 ‘9’s)
Access to Internet	Intermittent to independent	Persistent to interrupted
Response to Failure	Resilient, fail-in-place	Retry, replace
Network Topology	Federations of peer-to-peer	Constellations of peripherals
Physical Connectivity	Legacy & purpose-built	Evolving broadband & wireless
Example Gateways	Commercial monitoring *Echelon SmartServer*	Consumer home automation *Revolv Hub*

Interaction Style	Event Driven, Pub-Sub	Request / Response

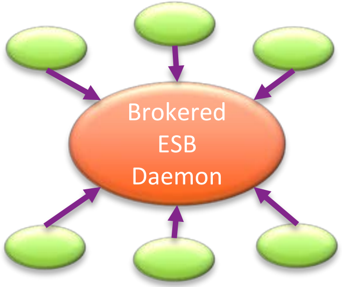
Data-Centric is Different!

Point-to-Point
Client/Server



TCP, REST, WS*, OPC

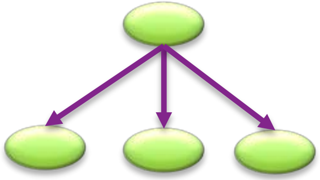
Brokered
Publish/Subscribe
Queuing



Brokered
ESB
Daemon

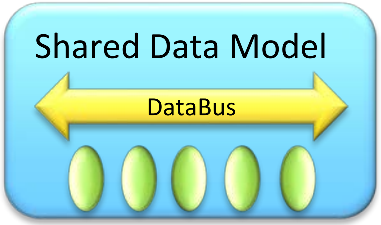
MQTT, XMPP, AMQP

Broadcast
Publish/Subscribe



Fieldbus, CANbus

Data-Centric
Publish-Subscribe



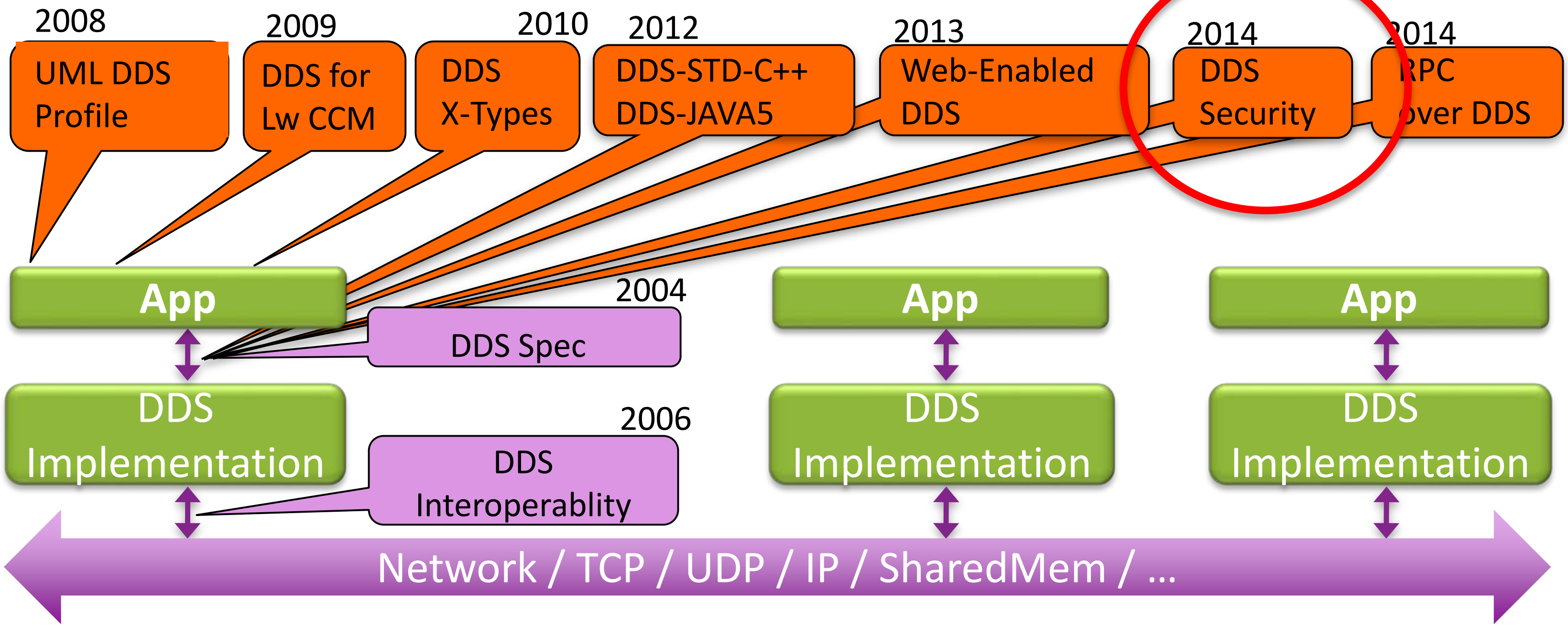
Shared Data Model

DataBus

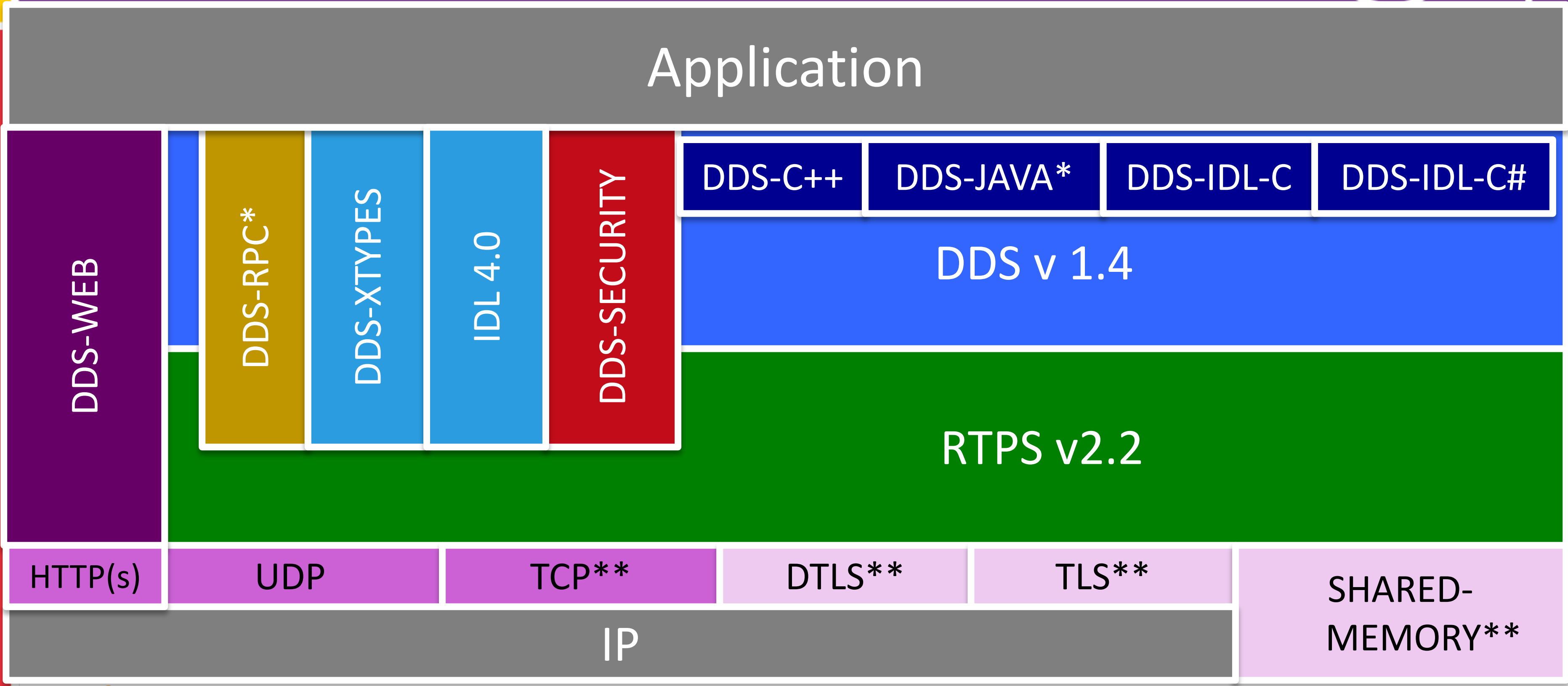
DDS

Data-Centric Middleware Standards

OMG Compliant DDS: Data Centric Messaging

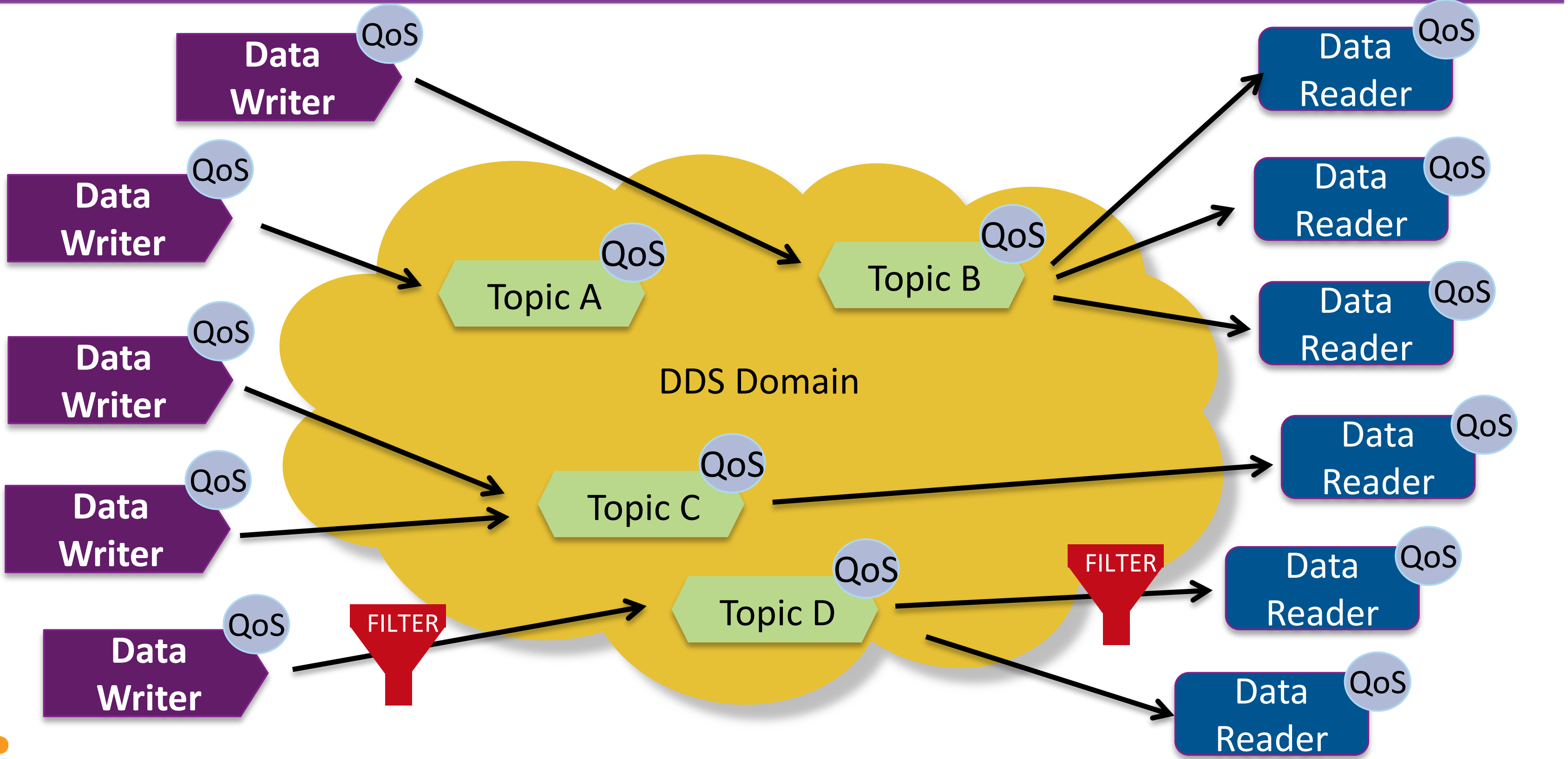


DDS Standards: Layered View

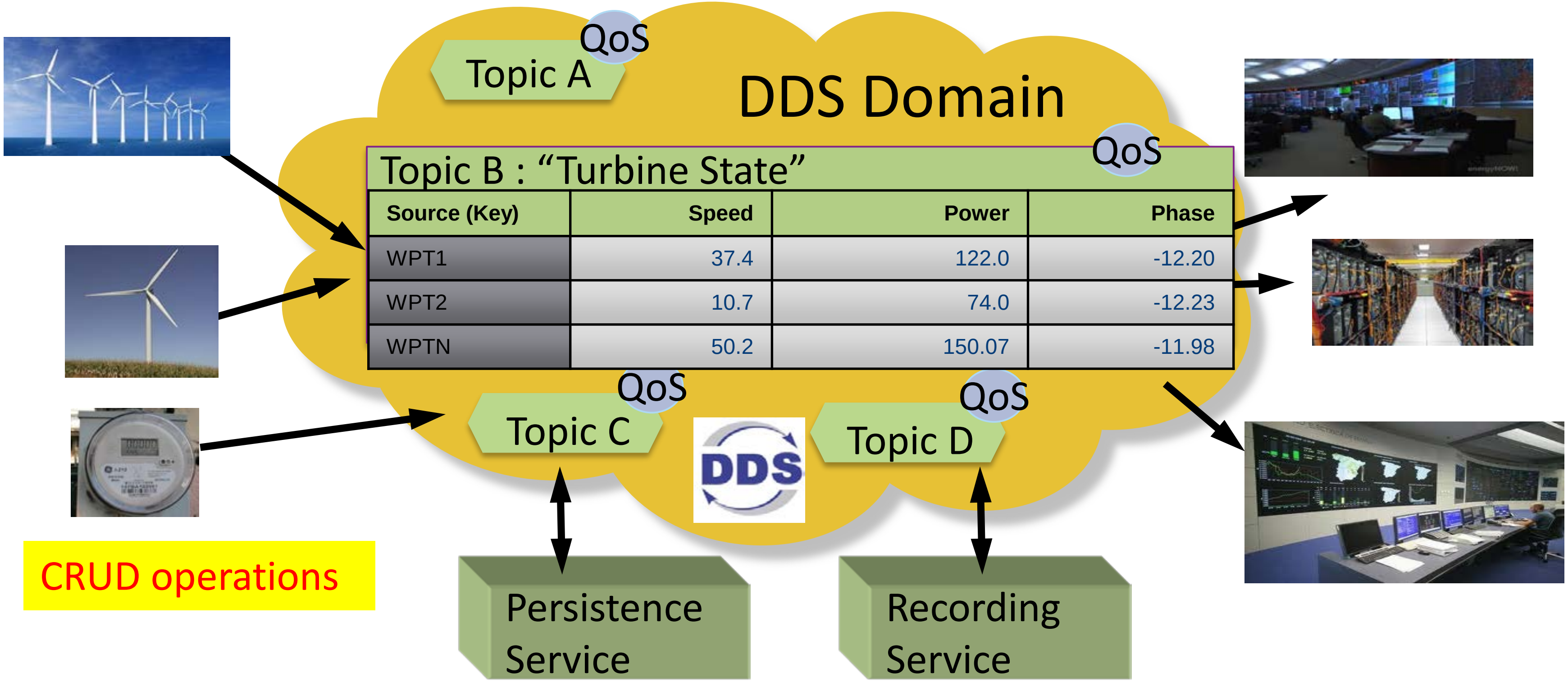


DDS Interoperability Workfest

Data Centricity



Virtual Global Data Space

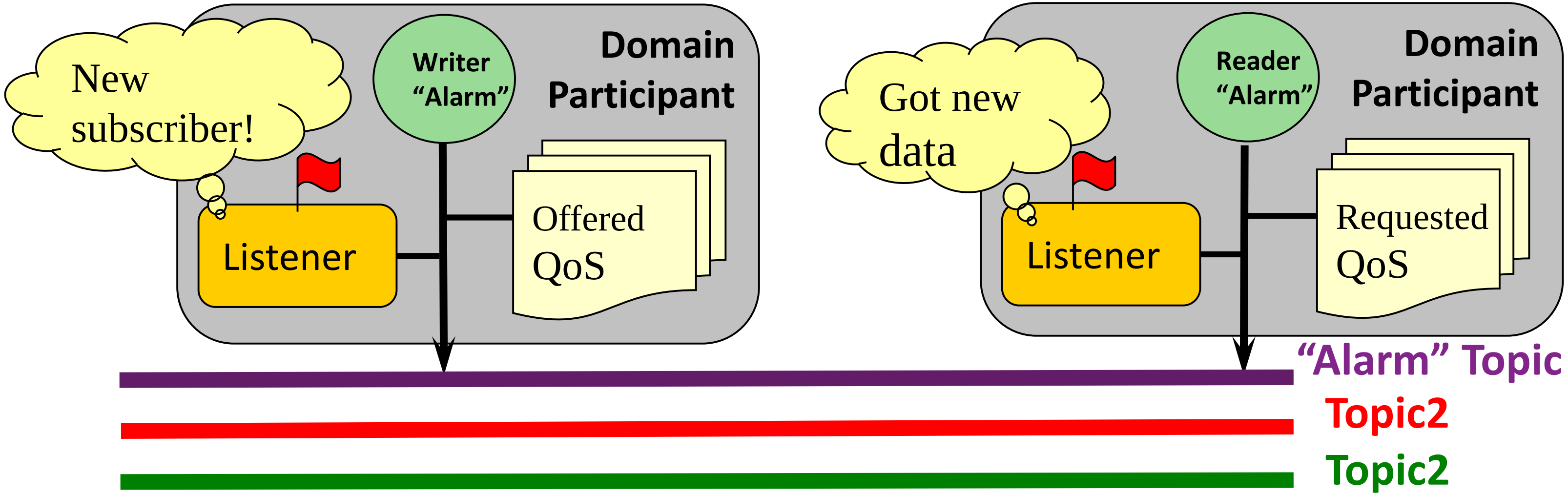


Topic B : “Turbine State”

Source (Key)	Speed	Power	Phase
WPT1	37.4	122.0	-12.20
WPT2	10.7	74.0	-12.23
WPTN	50.2	150.07	-11.98

CRUD operations

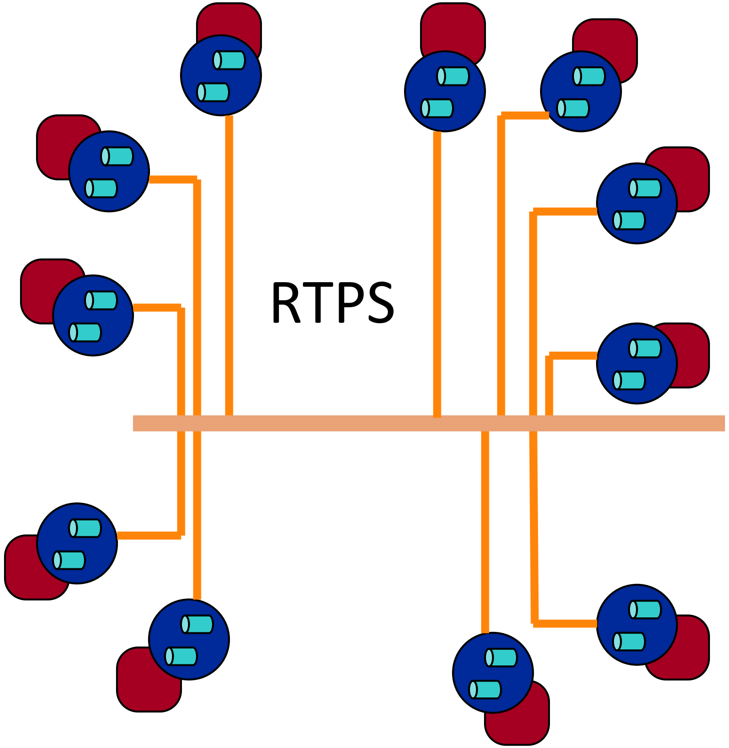
Data Centric Communications Model



Participants scope the global data space (domain)
Topics define the data-objects (collections of subjects)
DataWriters publish data on Topics
DataReaders subscribe to data on Topics
QoS Policies are used configure the system
Listeners are used to notify the application of events

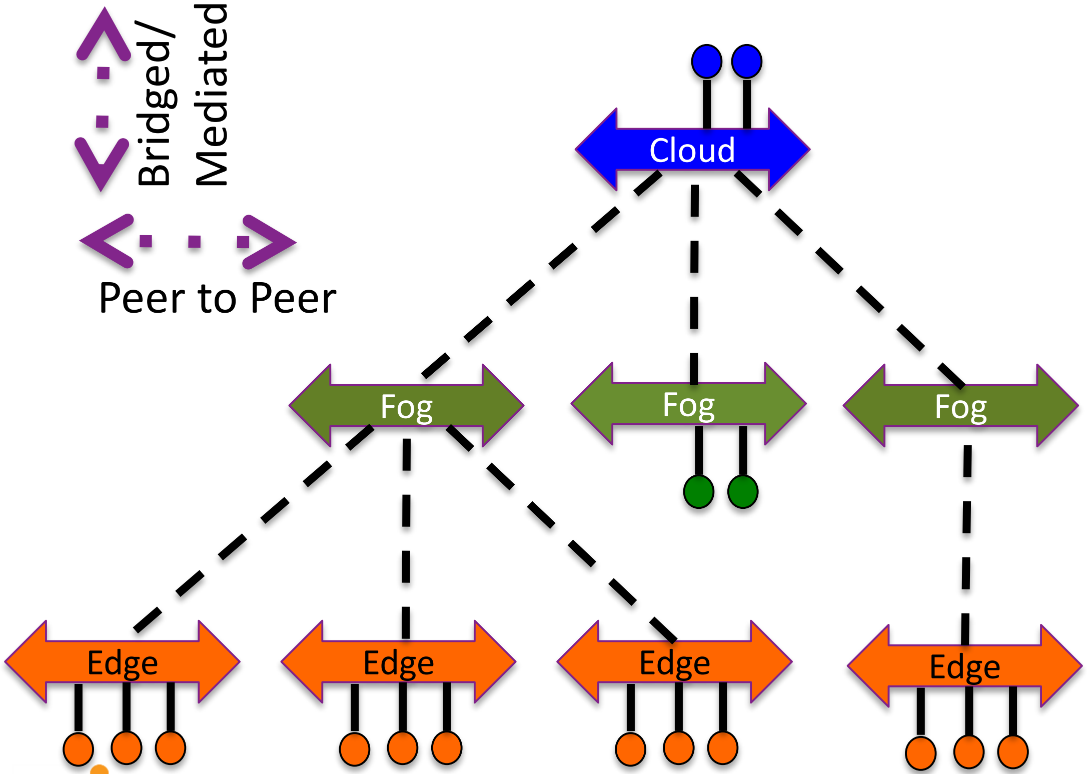
RTPS: Wire Protocol Optimized for IIoT

- Peer to peer: no brokers or servers
- Adaptable QoS, including prioritization
- Reliable even over multicast!
- Any size data automatic fragmentation
- Automatic Discovery and Presence
- Decoupled execution start in any order
- Redundant sources, sinks, paths, networks
- Efficient data encapsulation
- High performance: native “wire” speeds
- Scalable: no N^2 network connections



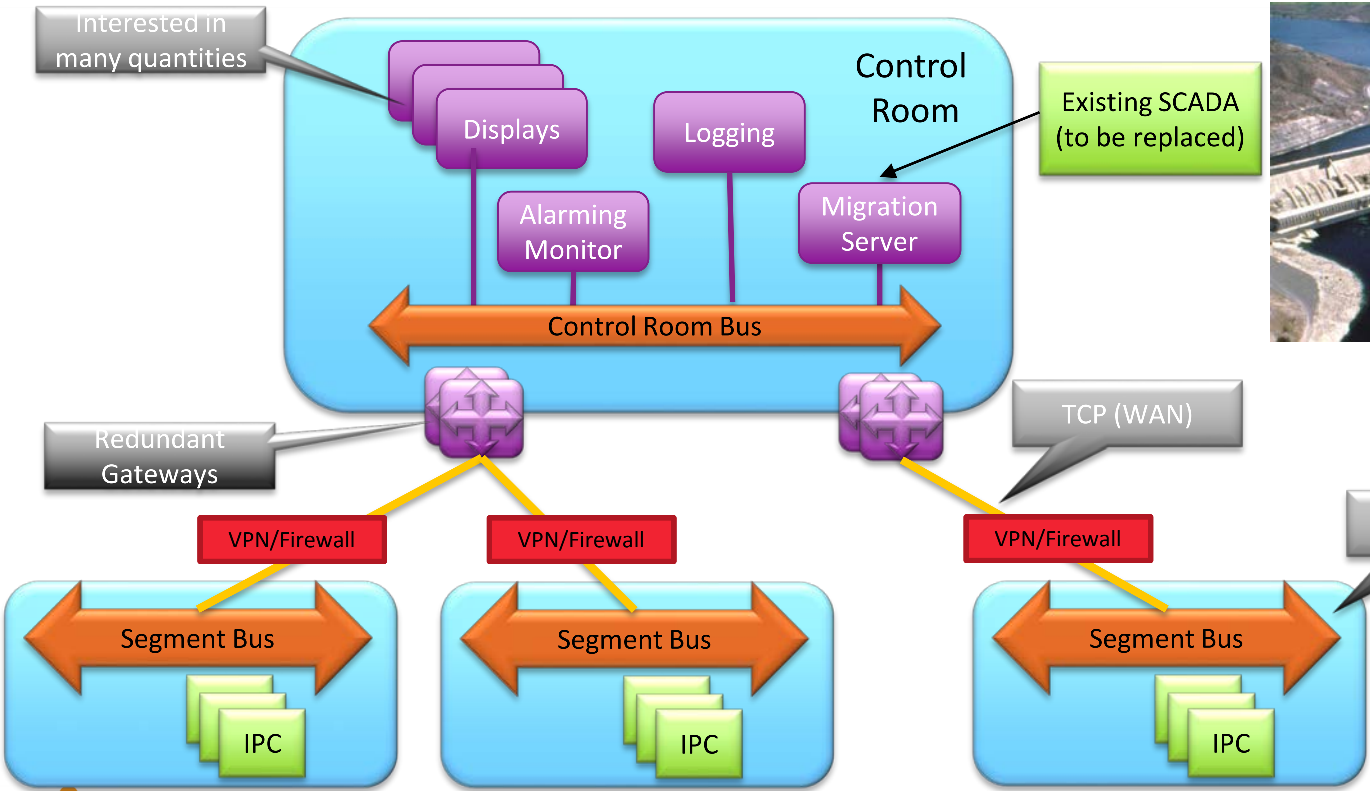
Deployment

Edge to Fog to Cloud

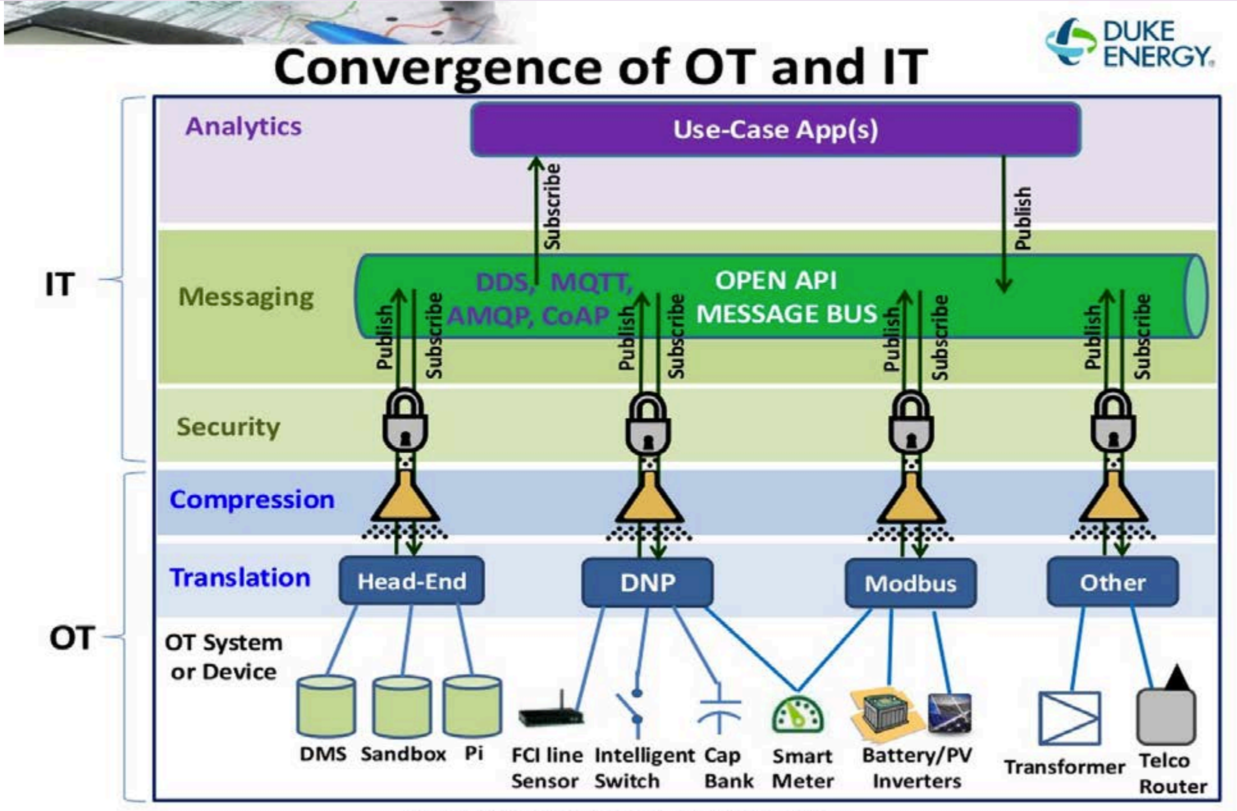


- Cloud:
  - Datacenter
  - Elasticity, Provisioning, Management, Analytics
- Fog:
  - Distributed computing
  - Processing "close to the edge"
  - Latency, Robustness, availability
- Edge:
  - Locality
  - Information Scoping

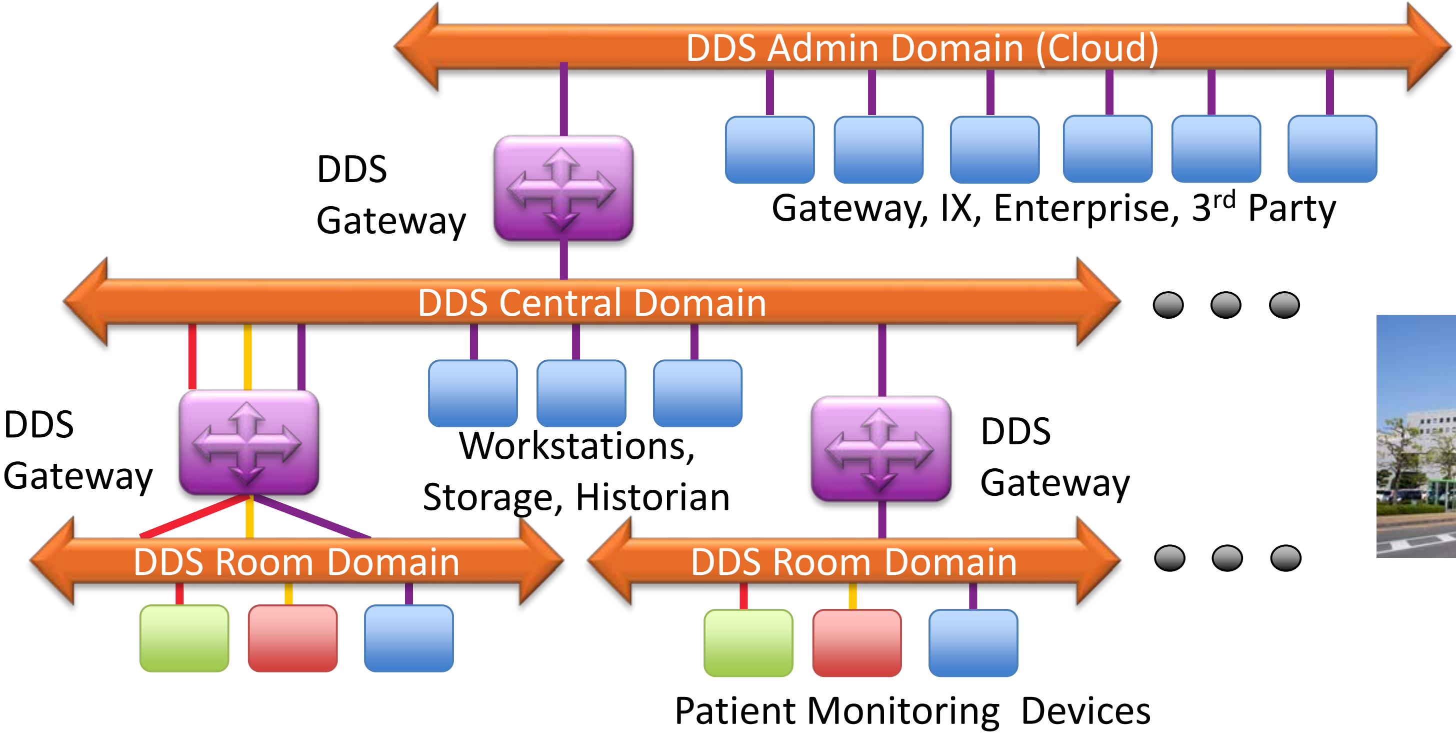
Example: GCD Ultra Available Plant Control



Example: Duke Energy



Example: Clinical Decision Support System Architecture



Introduction To Data Distribution Service Security

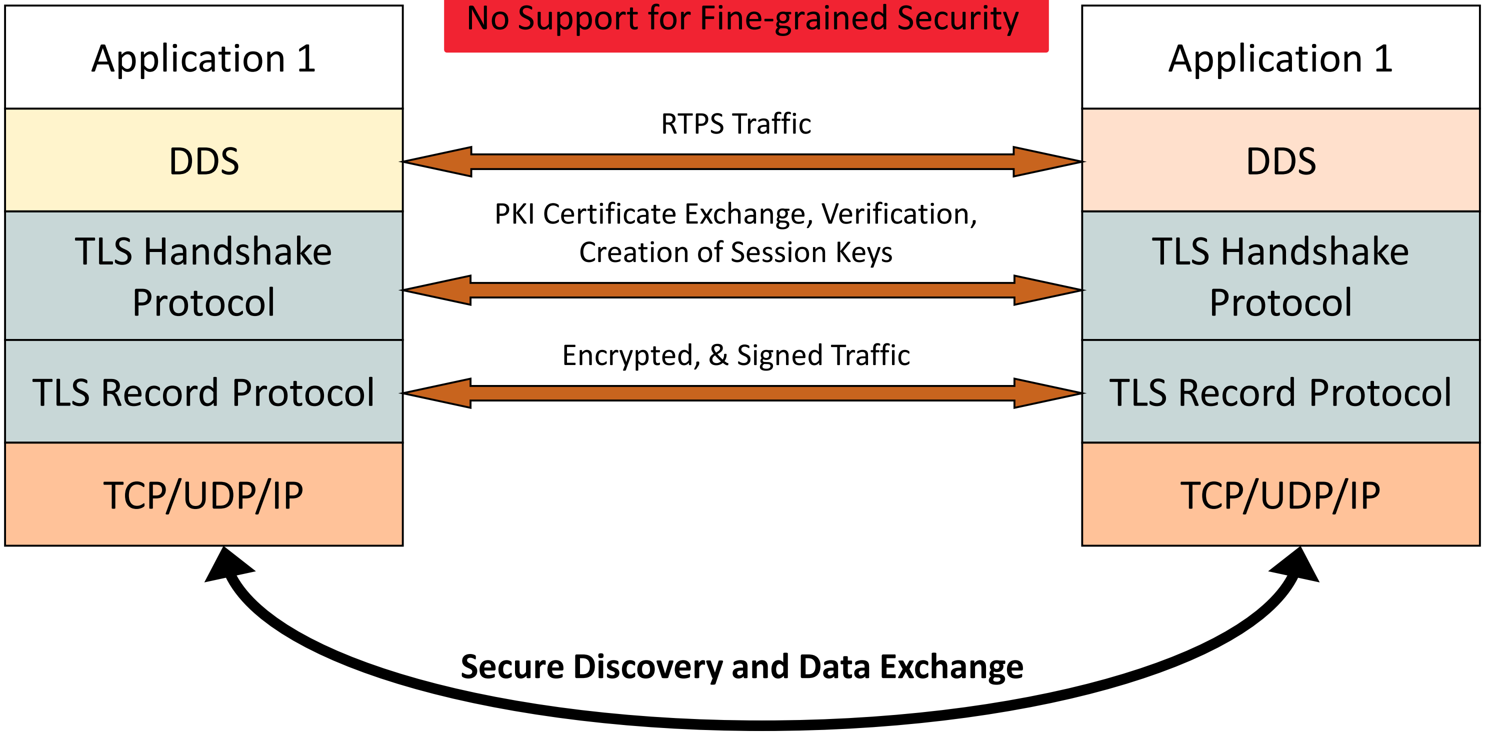
Hamed Soroush, Ph.D
Senior Research Security Engineer
Real-Time Innovations (RTI)
@HamedSoroush

Approaches to Protect DDS

- Transport Layer Security
- Fine-Grained Security

Transport Level Security

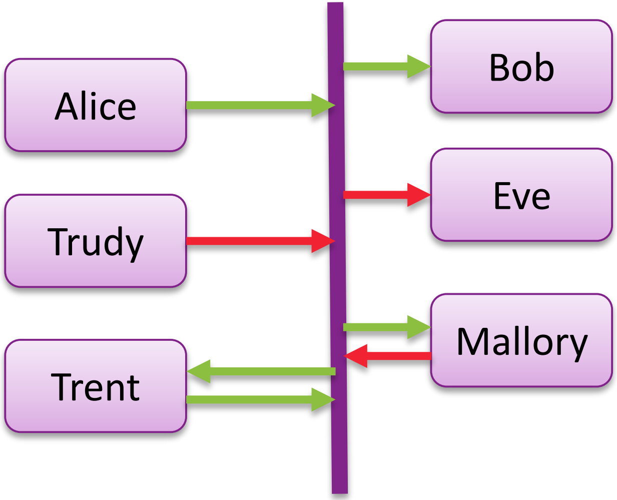
No Multicast Support
No Support for Fine-grained Security



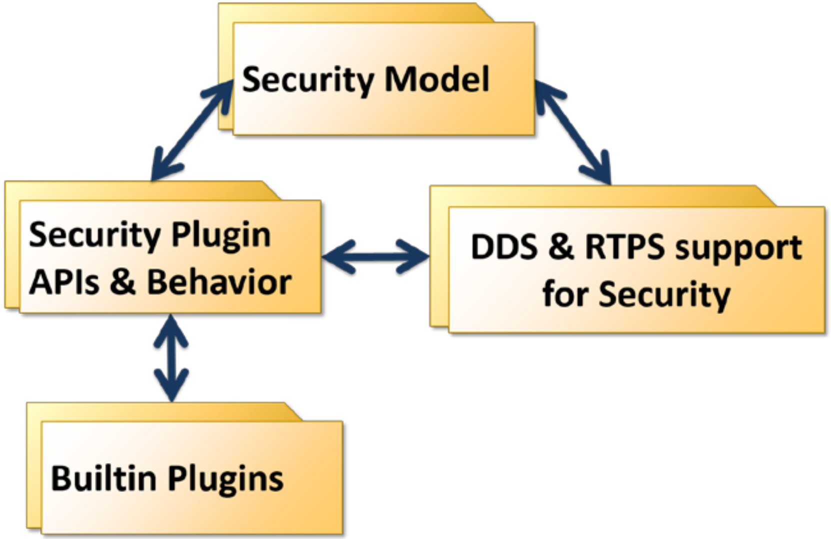
Threats

- Unauthorized Subscription
- Unauthorized Publication
- Tampering & Replay

Local machine is assumed to be trusted



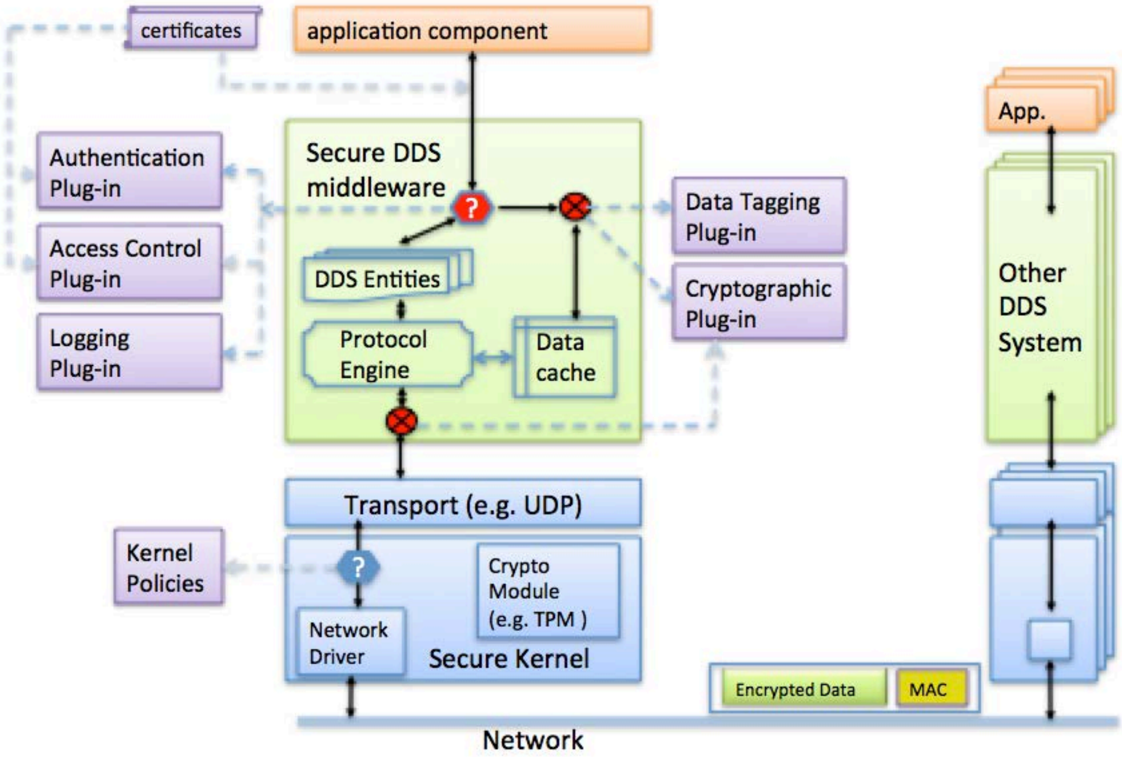
DDS Security Specification


Security Model
Security Plugin APIs & Behavior
DDS & RTPS support for Security
Builtin Plugins

DDS Security Model

Concept	Unix File System Security Model	DDS Security Model
Subject	User Process executing for a user	DomainParticipant Application joining a DDS domain
Protected Objects	Directories Files	Domain (by domain_id) Topic (by Topic name) DataObjects (by Instance/Key)
Protected Operations	Directory.list, Directory.create (File, Dir) Directory.remove (File, Dir) Directory.rename (File, Dir) File.read, File.write, File.execute	Domain.join Topic.create Topic.read (includes QoS) Topic.write (includes QoS) Data.createInstance Data.writeInstance Data.deleteInstance
Access Control Policy Control	Fixed in Kernel	Configurable via Plugin
Builtin Access Control Mode	**Per-File/Dir** Read/Write/Execute permissions for OWNER, GROUP, USERS	**Per-DomainParticipant** Permissions : What Domains and Topics it can JOIN/READ/WRITE

Pluggable Security Architecture



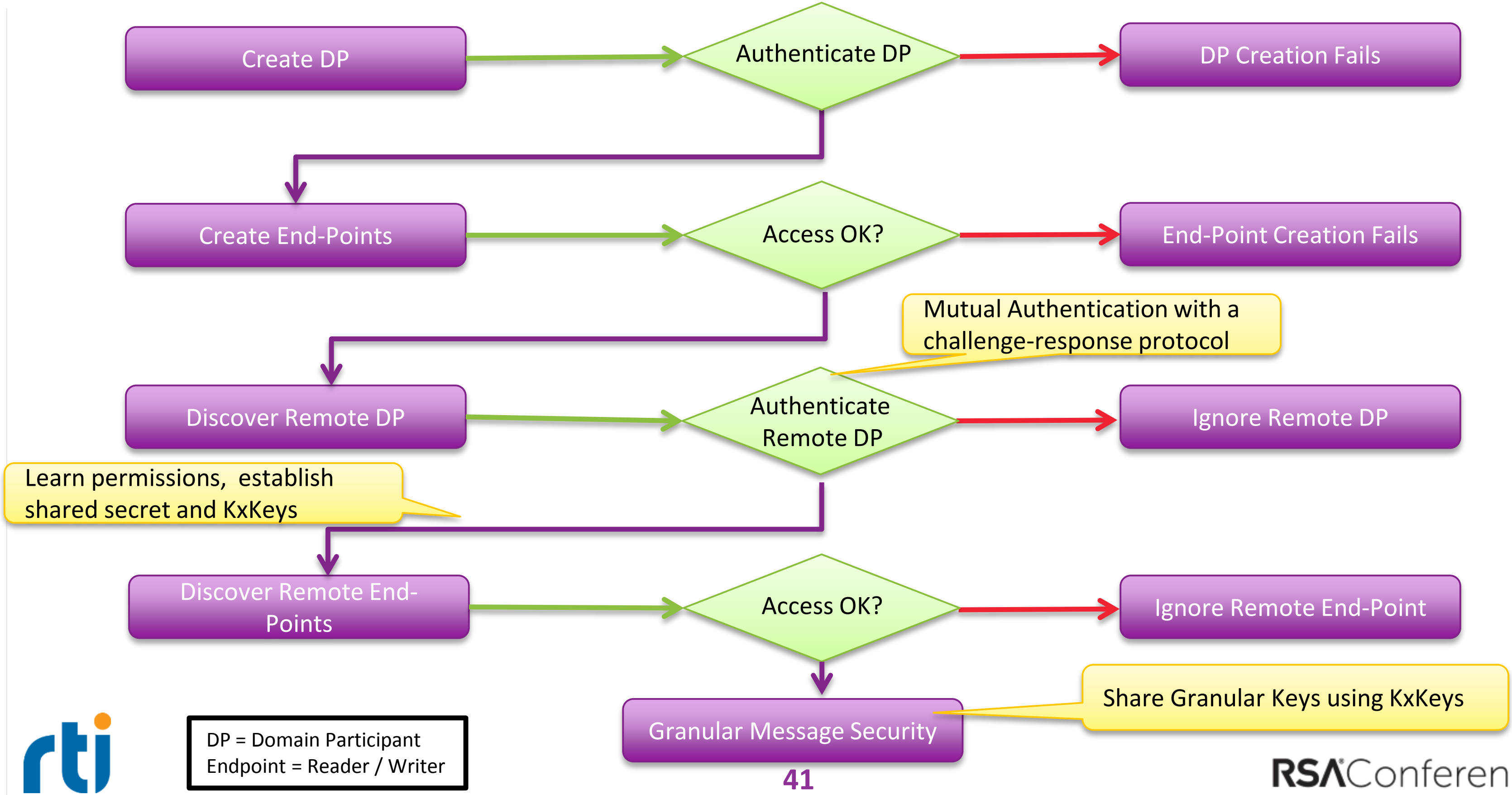
Pluggable Security Architecture

Plugin	Purpose	Interactions
Authentication	Authenticate the principal that is joining a DDS Domain. **Handshake and establish shared secret between participants**	The principal may be an application/process or the user associated with that application or process. Participants may send messages to do mutual authentication and establish shared secret
Access Control	Decide whether a principal is allowed to perform a protected operation.	Protected operations include joining a specific DDS domain, creating a Topic, reading a Topic, writing to a Topic
Cryptography	Perform the encryption and decryption operations. Create & Exchange Keys. Compute digests, compute and verify Message Authentication Codes. Sign and verify signatures of messages.	Invoked by DDS middleware to encrypt data compute and verify MAC, compute & verify Digital Signatures
Logging	Log all security relevant events	Invoked by middleware to log
Data Tagging	Add a data tag for each data sample	Can be used for access control

Standard Capabilities (Built-in Plugins)

Authentication	X.509 Public Key Infrastructure (PKI) with a pre-configured shared Certificate Authority (CA) RSA or ECDSA Signature Algorithm for authentication, DH or ECDH for shared secret
Access Control	Configured by domain using a (shared) Governance file Specified via permissions file signed by shared CA Control over ability to join systems, read or write data topics
Cryptography	Protected key distribution AES128-GCM and AES256-GCM for authenticated encryption AES128-GMAC or AES256-GMAC for message authentication and integrity
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 DDS

Overview of What Happens


Create DP
Authenticate DP
DP Creation Fails
Create End-Points
Access OK?
End-Point Creation Fails
Mutual Authentication with a challenge-response protocol
Discover Remote DP
Authenticate Remote DP
Ignore Remote DP
Learn permissions, establish shared secret and KxKeys
Discover Remote End-Points
Access OK?
Ignore Remote End-Point
Granular Message Security
Share Granular Keys using KxKeys

DP = Domain Participant
Endpoint = Reader / Writer

Writer Message Security

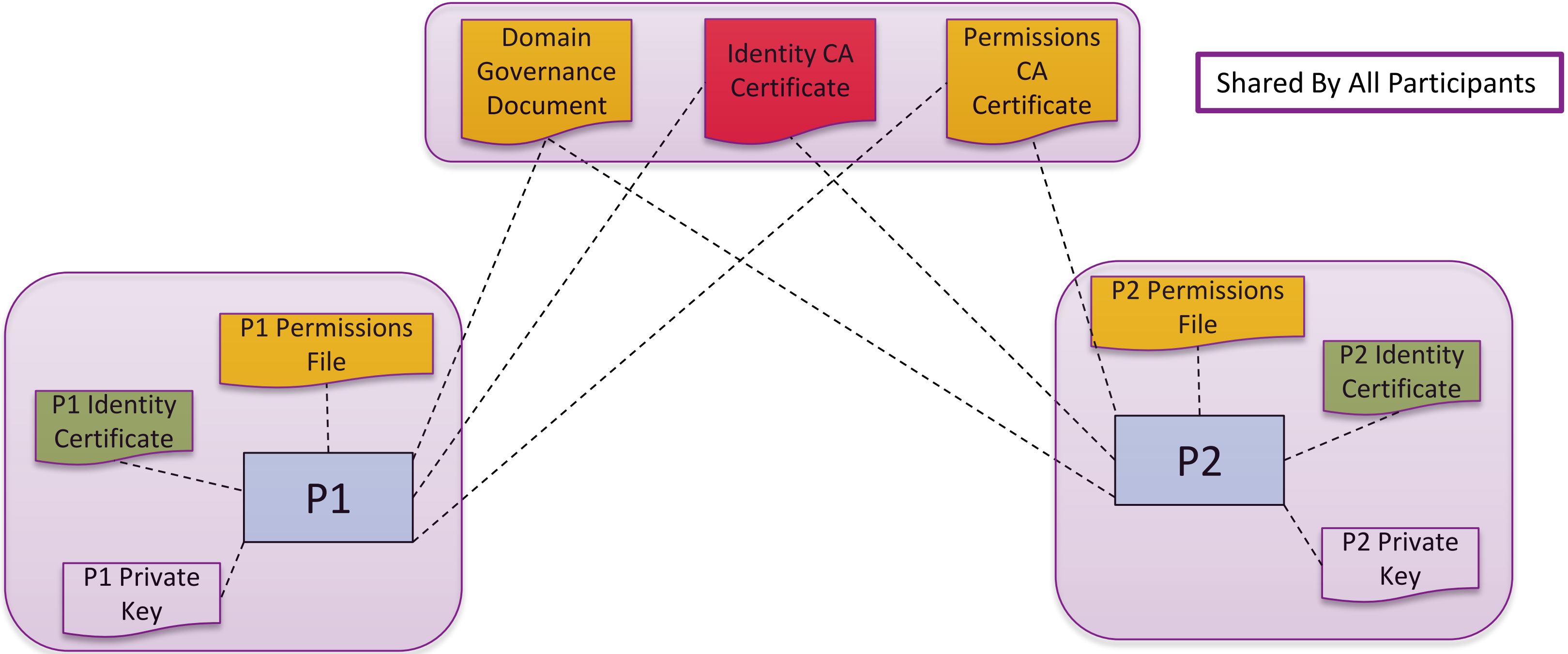
- Encryption keys & MAC keys are generated per data writer
- These keys are securely distributed to data readers
- Distribution of these keys is done using other symmetric keys derived from the shared secret
  - Key distribution is transport independent
- Different parts of messages can optionally be protected per governance policy
- Data Delivery is independent of key distribution
  - May use any transport, including multicast

Access Control & Policy

- DDS Security allows for configuring & enforcing the privileges of each participant
  - Which domains it can join & what Topics it can read/write
- It also allows specifying & enforcing policies for the whole domain, e.g.
  - Which topics are discovered using Secure Discovery
  - Which Topics have controlled access
  - Encrypt or Sign for Secure Discovery
  - Encrypt or Sign for each secure Topic
  - What to do with unauthenticated access requests

DDS Security: Out-of-the-Box

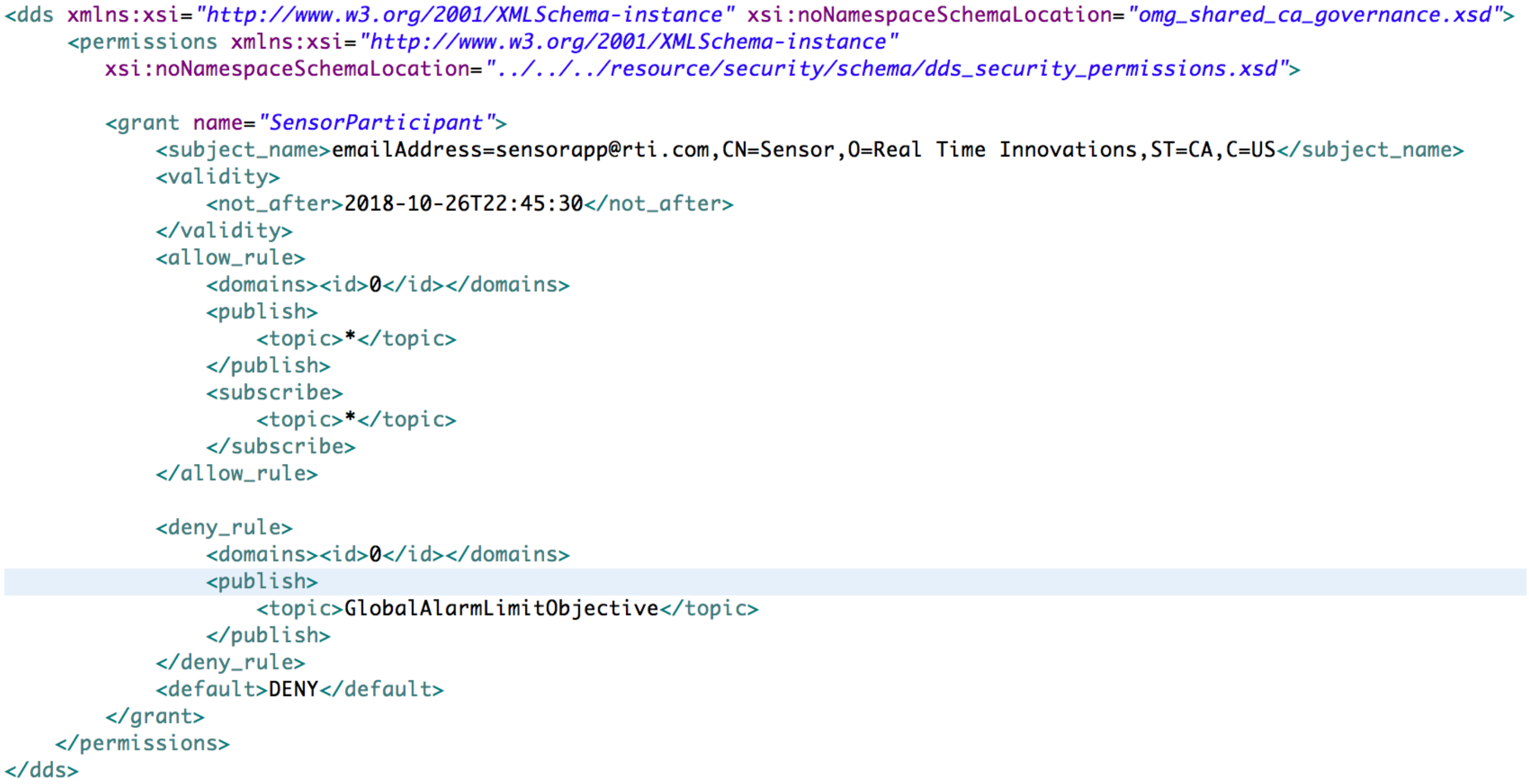
Configuring & Deploying DDS Security



Permissions Document

- For each participant specifies:
  - What domains it can join
  - What Topics it can read/write
  - What Tags are associated with Readers & Writers

A Sample Permissions File

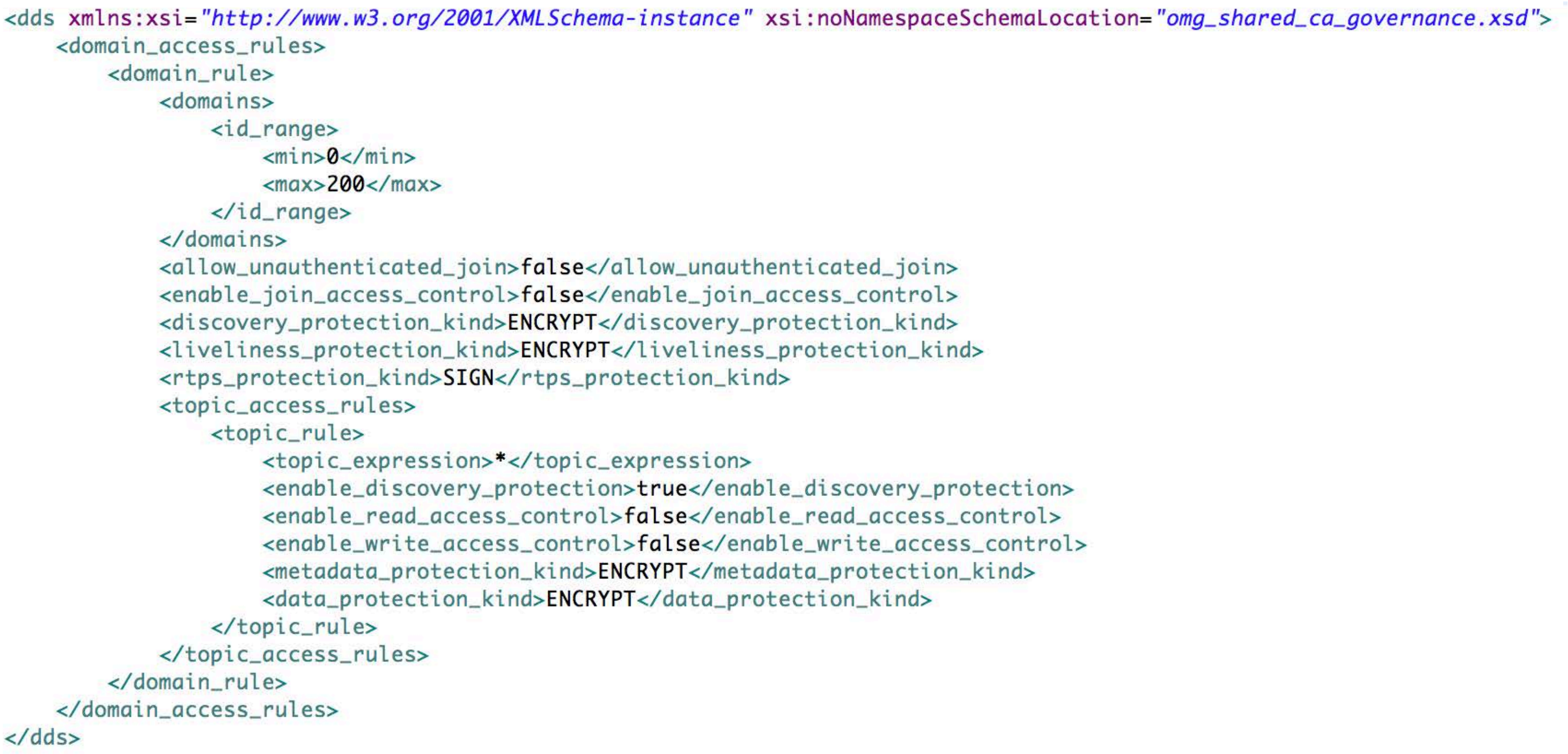


```
<dds xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="omg_shared_ca_governance.xsd">
     <permissions xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:noNamespaceSchemaLocation="../../../resource/security/schema/dds_security_permissions.xsd">

        <grant name="SensorParticipant">
            <subject_name>emailAddress=sensorapp@rti.com,CN=Sensor,O=Real Time Innovations,ST=CA,C=US</subject_name>
            <validity>
                <not_after>2018-10-26T22:45:30</not_after>
            </validity>
            <allow_rule>
                <domains><id>0</id></domains>
                <publish>
                    <topic>*</topic>
                </publish>
                <subscribe>
                    <topic>*</topic>
                </subscribe>
            </allow_rule>

            <deny_rule>
                <domains><id>0</id></domains>
                <publish>
                    <topic>GlobalAlarmLimitObjective</topic>
                </publish>
            </deny_rule>
            <default>DENY</default>
        </grant>
    </permissions>
</dds>
```

Domain Governance File

- The domain governance document is an XML document that specifies which DDS domain IDs shall be protected and the details of the protection.
- It is signed by the permissions CA.

A Sample Governance File



```
<dds xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:noNamespaceSchemaLocation="omg_shared_ca_governance.xsd">
    <domain_access_rules>
        <domain_rule>
            <domains>
                <id_range>
                    <min>0</min>
                    <max>200</max>
                </id_range>
            </domains>
            <allow_unauthenticated_join>false</allow_unauthenticated_join>
            <enable_join_access_control>false</enable_join_access_control>
            <discovery_protection_kind>ENCRYPT</discovery_protection_kind>
            <liveliness_protection_kind>ENCRYPT</liveliness_protection_kind>
            <rtps_protection_kind>SIGN</rtps_protection_kind>
            <topic_access_rules>
                <topic_rule>
                    <topic_expression>*</topic_expression>
                    <enable_discovery_protection>true</enable_discovery_protection>
                    <enable_read_access_control>false</enable_read_access_control>
                    <enable_write_access_control>false</enable_write_access_control>
                    <metadata_protection_kind>ENCRYPT</metadata_protection_kind>
                    <data_protection_kind>ENCRYPT</data_protection_kind>
                </topic_rule>
            </topic_access_rules>
        </domain_rule>
    </domain_access_rules>
</dds>
```

Configuration Possibilities

- Are “legacy” or un-identified applications allowed in the Domain?
  - If yes an unauthenticated applications will:
    - See the “unsecured” discovery Topics
    - Be allowed to read/write the “unsecured” Topics
- Is a particular Topic discovered over protected discovery?
  - If so it can only be seen by “authenticated applications”
- Is access to a particular Topic protected?
  - If so only authenticated applications with the correct permissions can read/write
- Is data on a particular Topic protected? How?
  - If so data will be sent signed or, encrypted then signed
- Are all protocol messages signed? Encrypted?
  - If so only authenticated and authorized applications will see anything

Hands-On Session

Rose Wahlin

Principal Software Engineer

Real-Time Innovations (RTI)

@ProjectDerby

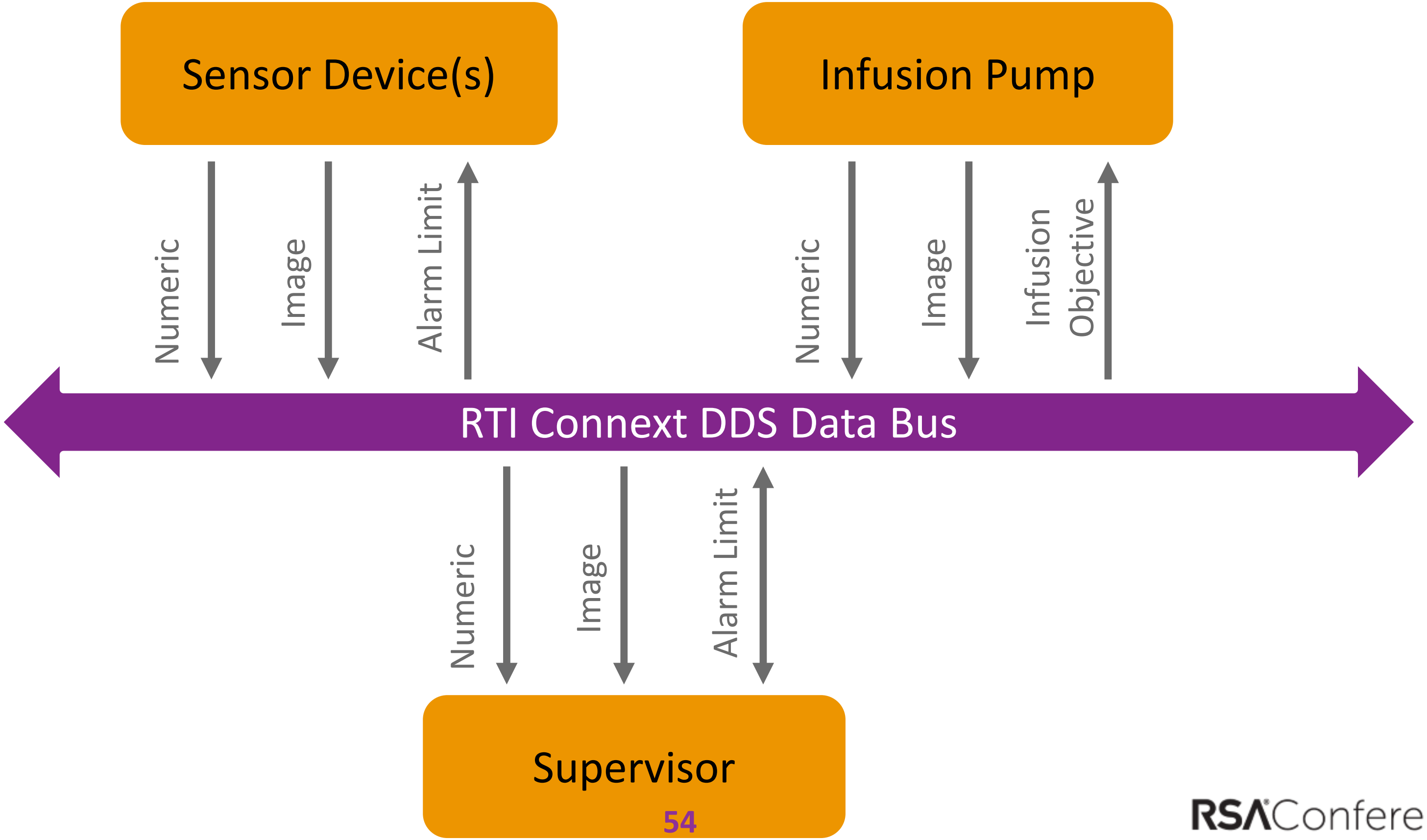
What Are we Doing?

- Three scenarios:
  - Understanding the system with no security
  - Securing the system with transport-level security
  - Securing the system with fine-grained access control

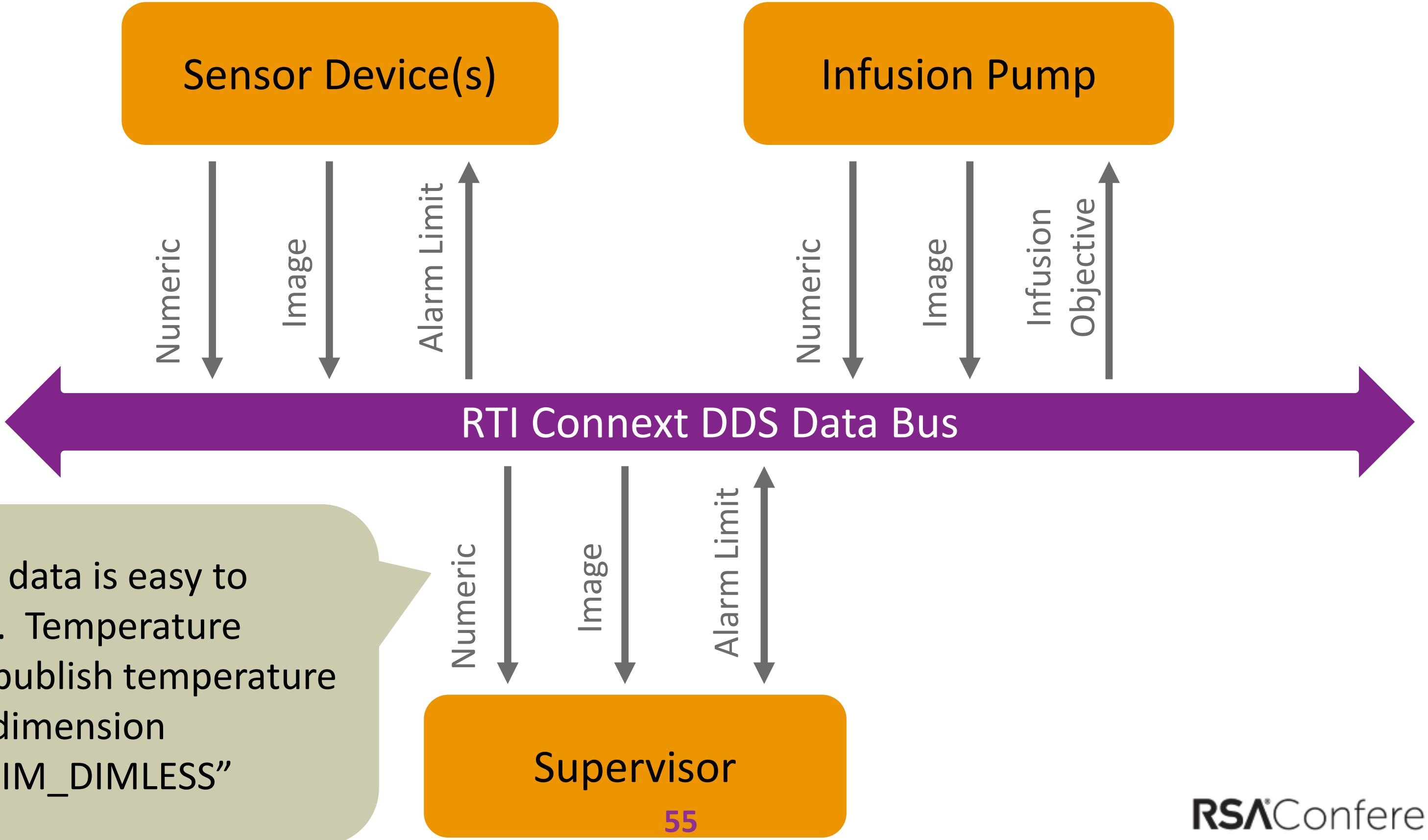
What is in this System?

- Sensor devices
  - Static data about the device: Device ID, Image
  - Data: Numeric
  - (Etc.)
- Infusion pump
  - Sensor device with additional status and a stop command called “InfusionObjective”
- Supervisor
  - Receives all the sensor data and infusion pump status
  - Sends and receives alarm limits – used to detect whether a patient’s vitals are bad enough to show an alarm
  - Sends the InfusionObjective command to the infusion pump

System Overview

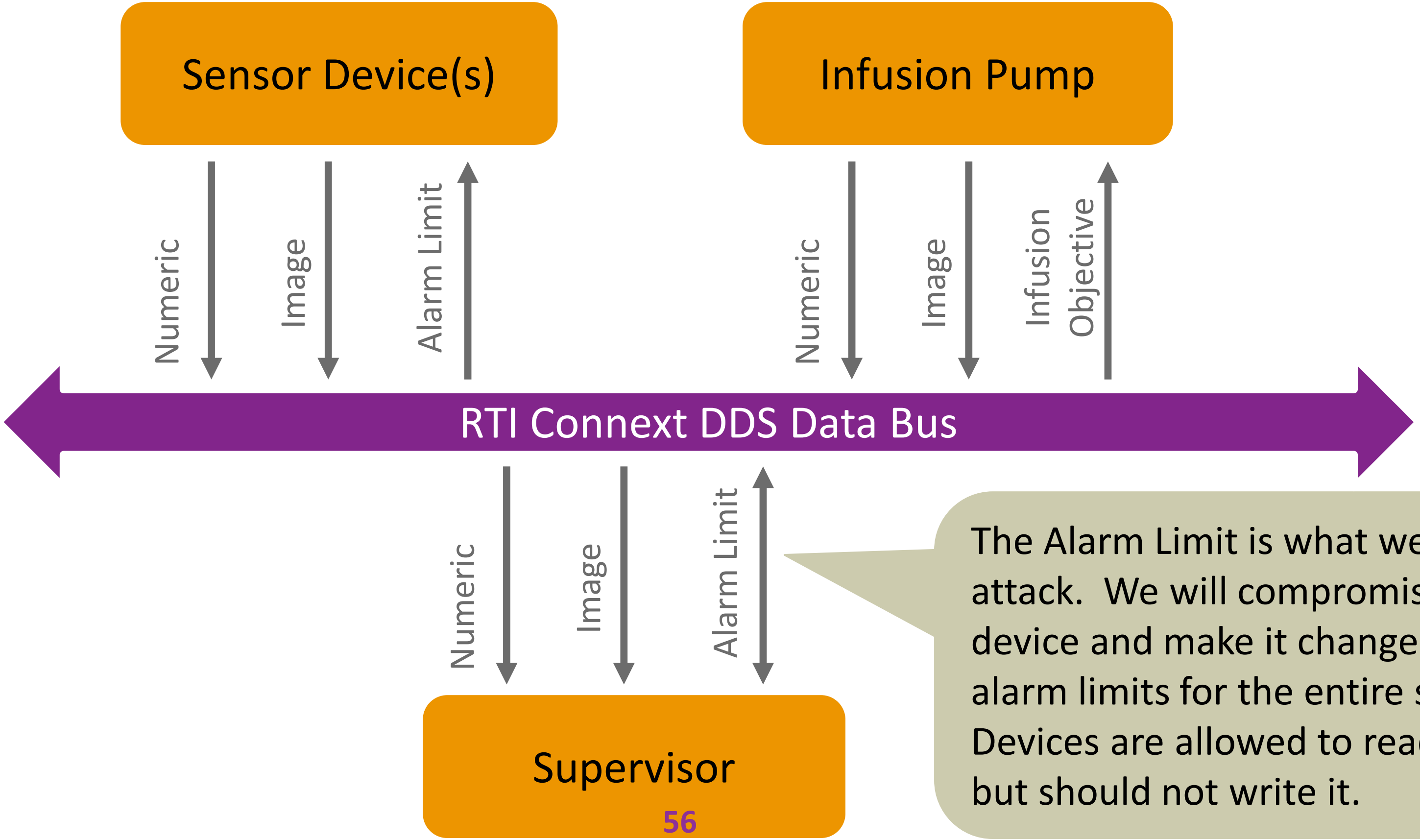


Exercise 1: Viewing Unsecured Data



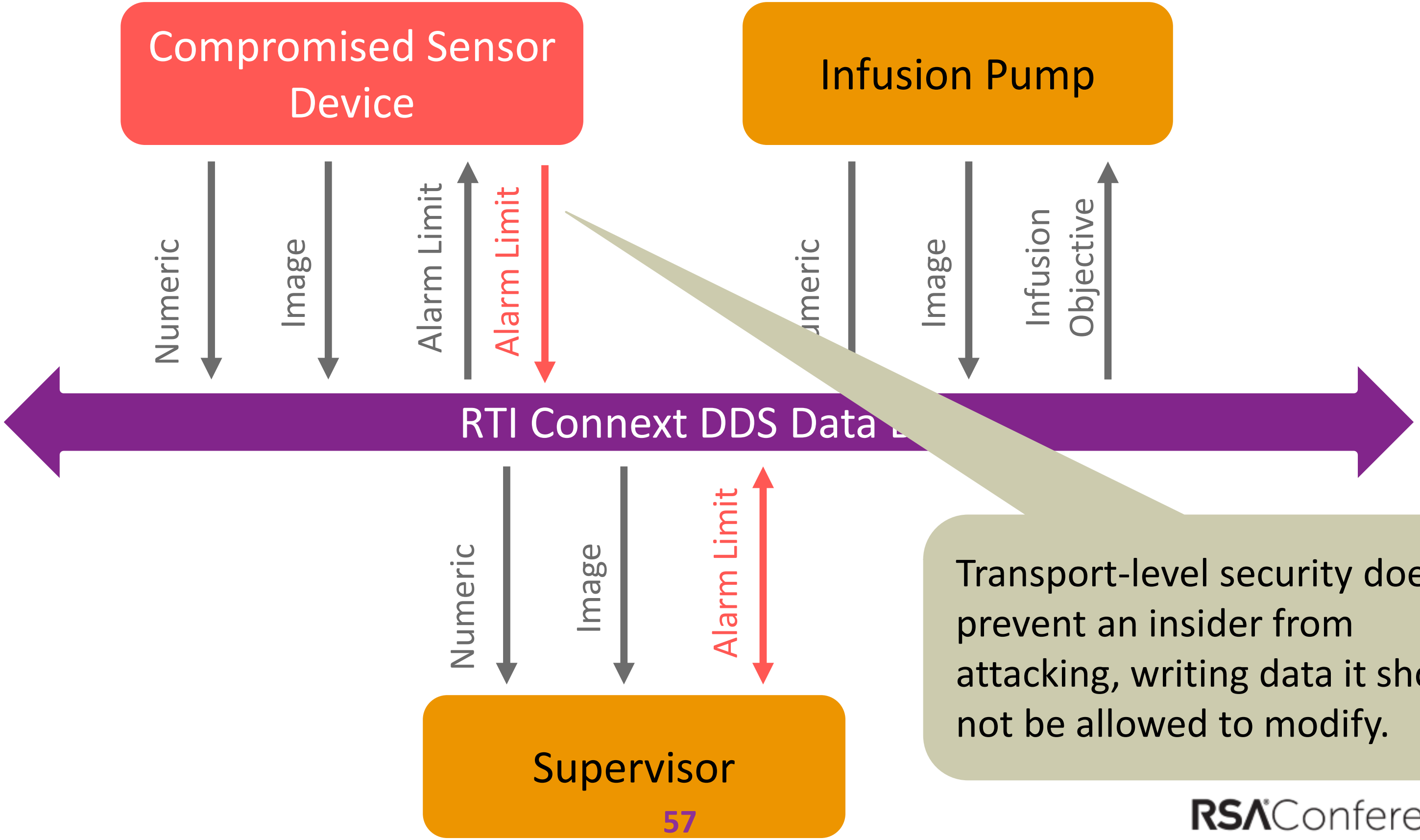
Numeric data is easy to visualize. Temperature sensors publish temperature 37, and dimension “MDC_DIM_DIMLESS”

Exercise 2: Transport-Level Security



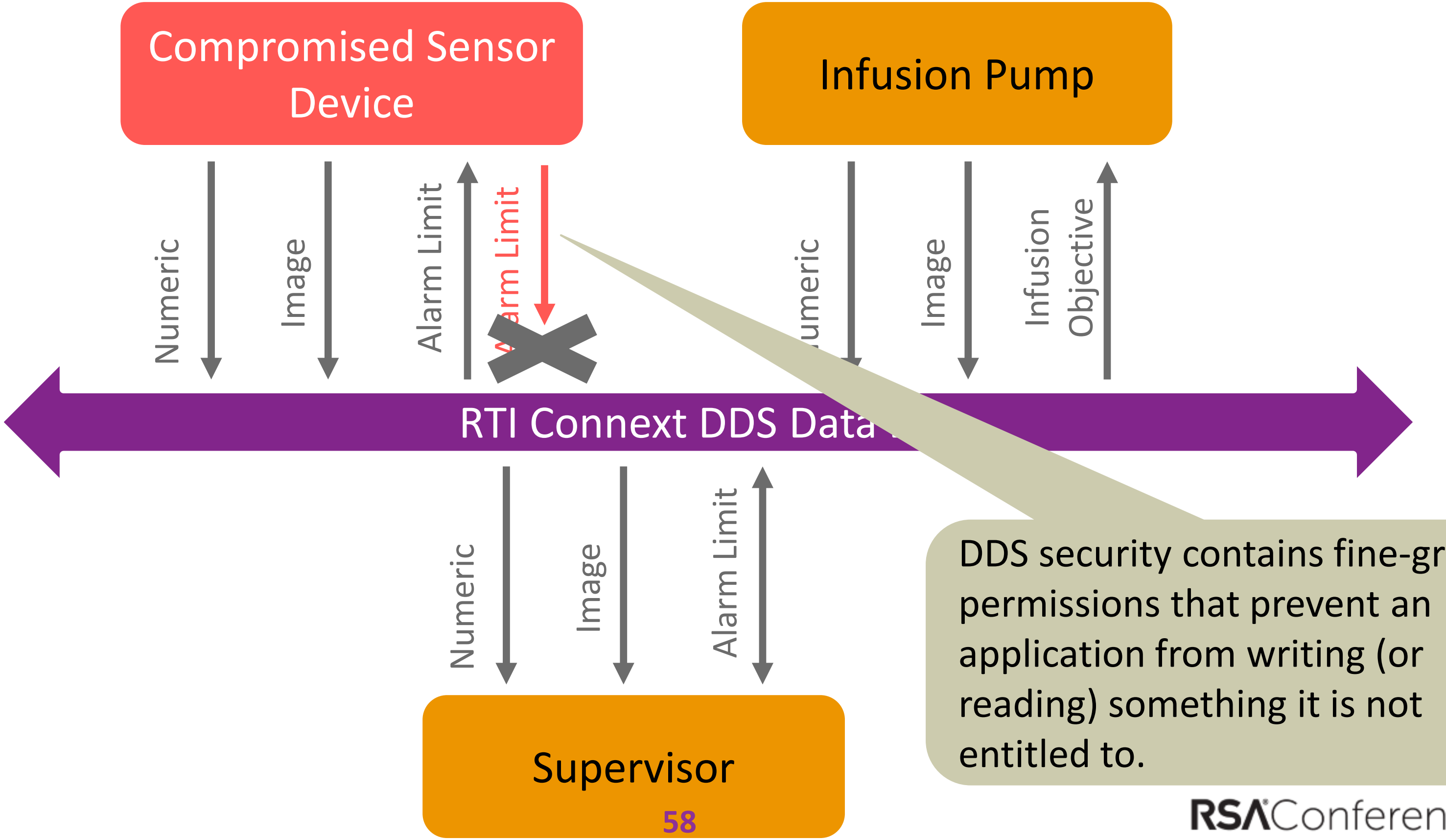
The Alarm Limit is what we will attack. We will compromise a device and make it change the alarm limits for the entire system. Devices are allowed to read this, but should not write it.

Exercise 2: Transport-Level Security



Transport-level security does not prevent an insider from attacking, writing data it should not be allowed to modify.

Exercise 3: Permissions



DDS security contains fine-grained permissions that prevent an application from writing (or reading) something it is not entitled to.

Concluding Remarks

Try out DDS Security

- Current Specification Draft:
  - http://www.omg.org/spec/DDS-SECURITY/
- Any Questions?
  - https://community.rti.com/

“Apply”

- Conduct an assessment of the security posture of your system, including network communication protocols
- Identify network protocols that you are using and associated risks
  - You will need granular security for
    - Better performance (e.g. selective encryption/authentication of messages)
    - More resilience (e.g. better protection against insiders)
- Learn more about standard Industrial Internet technologies, including
    - IIC’s Industrial Internet Reference Architecture
    - IIC’s Industrial Internet Security Framework Document
    - IIC’s Industrial Internet Connectivity Reference Architecture

References

- Industrial Internet Consortium
  - http://www.iiconsortium.org/
- Object Management Group’s DDS Portal
  - http://portal.omg.org/dds