WHITEPAPER

Four Keys to Securing Distributed Control Systems

EXECUTIVE SUMMARY

At the core of critical infrastructure and industrial applications, control systems drive today's power grid, hospital clinical environments, factories, vehicles, transportation systems and military operations. Because of their vital roles and the value of the information they exchange, these systems must be protected from both espionage and sabotage.

Security, however, has become more challenging. Millions of devices tap into today's Industrial Internet of Things. More connections translate into more points of vulnerability, but security must not compromise other fundamental requirements including reliability, real-time performance, autonomy and interoperability.

This white paper presents an overview of industrial security requirements and the new security extensions to the Data Distribution Service (DDS) standard. Implemented as plug-ins, the security extensions introduce authentication, confidentiality and access control while still satisfying demanding reliability and performance requirements. A power grid use case shows how DDS Security can be easily incorporated into existing systems — with or without prior adoption of the foundational DDS standard.

CONTROL SYSTEMS

Industries that now depend on Internet connectivity cover the globe and relate to all aspects of modern life. As a result, the scope of the Internet has grown over time. The Industrial Internet of Things (Industrial Internet or IIoT) reflects the expanding requirements for connectivity at the heart of modern industry and commerce.

The control systems designed for the Industrial Internet have also evolved. Highly distributed in nature, a typical control system synthesizes live data streams from numerous sensors, actuators and other connected devices. Processed data then drives device control, and feeds other subsystems relating to operator interfaces, back-end systems, IT and cloud applications.

Because of their hierarchical nature, many modern control systems are referred to as "systems of systems." (Fig. 1.) These highly complex systems, with smarter devices at the lower levels and broadened information sharing at the upper levels, pose unique security challenges. System designers must meet those challenges without compromising other vital requirements relating to real-time performance, safety and reliability.

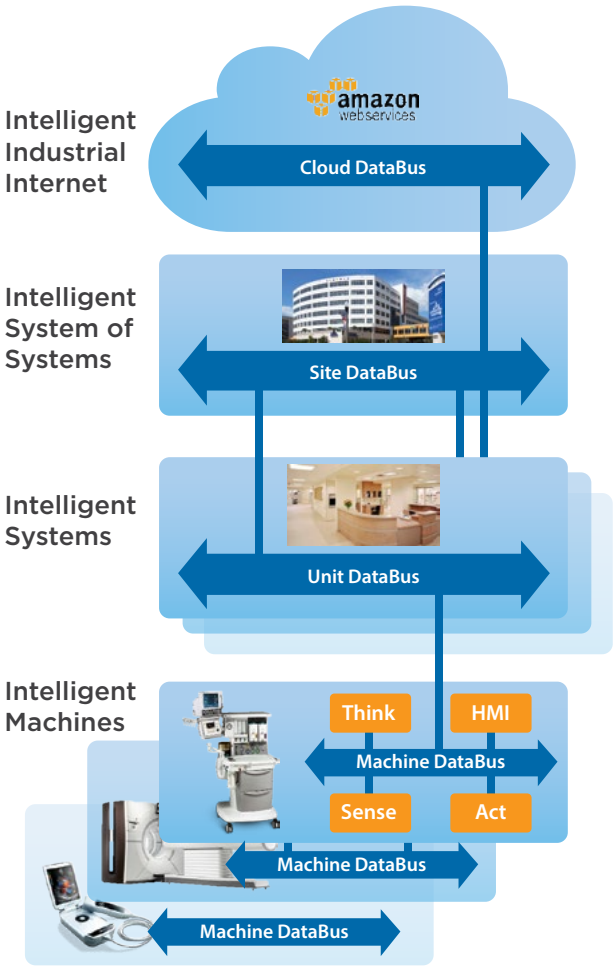

Figure 1. Within a modern hospital, the Industrial Internet connects intelligent medical devices at the bedside, in operating rooms and throughout all departments. The applications that aggregate data from these devices are themselves part of larger systems that drive up overall quality of care and save lives. Safeguarding patient health information and ensuring continuity of care requires security at every level of the hierarchy.

FOUR KEYS TO SECURING THE IIOT

A secure IIoT needs a decentralized architecture, access control, elimination of TCP/transport layer dependencies and interoperability.

DECENTRALIZED ARCHITECTURE

Industrial-strength data sharing can improve power generation and distribution, monitor and optimize use, and even power new business models and energy business systems.
Most traditional IT systems and consumer Internet of Things applications rely on centralized intelligence and message routing. However, a central broker or server would severely limit industrial control systems in terms of:

- Performance. A centralized messaging hub creates a bottleneck and choke point, which degrades latency and determinism as message volumes increase. Capacity and throughput are also constrained by the link speeds and switching performance at the hub.
- Scalability. The need to duplicate expensive hub servers drives up costs rapidly. Server cost grows with volume.
- Robustness. The hub creates a single point of failure or vulnerability, and system availability is directly tied to server maintenance and failures.
- Capabilities and utility. Centralized intelligence limits the autonomy and intelligence at the edge.

To overcome these limits, the vast majority of industrial control systems should adopt highly decentralized architectures. With distributed processing and more intelligence at the edge, overall systems can achieve lower latencies (faster throughput) and higher resiliency and can analyze orders of magnitude more data.

ACCESS CONTROL

Historically, physical site security or limited access to computer systems would serve to secure industrial control systems. Today, with much higher levels of system connectivity, machines are much more accessible. More people — authorized and unauthorized — are attempting to access those systems. Access controls have become critical for industrial systems, and must address the physical layer all the way up through the application software layers.

Without adequate security, systems are vulnerable to increased threats and attack activities. These include both espionage (unauthorized access) as well as sabotage of equipment and infrastructure. The required protection must target and prevent unauthorized subscription (eavesdropping), unauthorized publication (introducing invalid data and corrupting the behavior of the system), tampering and replay of information and unauthorized data access via infrastructure services.

ELIMINATING TCP/TRANSPORT LAYER DEPENDENCIES

At the transport layer, TCP provides no control over latency and lacks the control necessary for real-time behaviors. Since TCP is a unicast-only protocol, it also lacks the efficiency required in industrial environments that are traditionally multicast (one-to-many and many-to-many connections). TCP also assumes a reliable network, and can introduce a lot of overhead on less reliable networks.

IP can also be inefficient over very low-bandwidth networks such as satellite links. This protocol can also introduce too much overhead compared to other high-speed interconnects such as shared memory and RDMA.

In addition to latency issues, transport layer security built on top of TCP or IP inherits other shortcomings of these protocols, such as a lack of fine-grained access controls. Once a connection has been established (keys exchanged between peers), those peers can exchange any data without restrictions. To address this shortcoming, message brokers are often introduced in an IT or consumer environment to enforce policies. However, this then requires a centralized architecture that does not accommodate industrial systems.

INTEROPERABILITY (OPEN ARCHITECTURE)

Industrial systems encompass a broad range of components and subsystems from multiple vendors and must be supported over long lifecycles. Interoperability promotes modularity, which simplifies support of these components and therefore avoids spiraling costs over time.

Modular, interoperable components have become critical as system complexity has skyrocketed. Proprietary, hard-coded integration between components is impractical to maintain, difficult to evolve and limits design re-use. In contrast, well-defined interfaces and semantics simplify the evolution of very large scale systems.

DATA DISTRIBUTION SERVICE FOR THE IIOT

The Data Distribution Standard (DDS) emerged in conjunction with the evolution of the Industrial Internet of Things. For modern-day control systems, DDS addresses all four requirements for achieving secure, reliable, high-performance connectivity.

The standard provides connectivity between software modules, effectively creating a software DataBus.™ Well-defined interfaces and a standard interoperability protocol provide loose coupling between the modules in a system. The DDS protocol spans discovery (how modules locate each other), data routing, high-availability and real-time quality of service (QoS) enforcement.

The DDS application programming interface (API) enables portability across DDS implementations, and a DDS network wire protocol ensures interoperability. (See Fig. 2.) The standard also includes a discoverable data model. The DDS standard is published and managed by the Object Management Group (OMG).

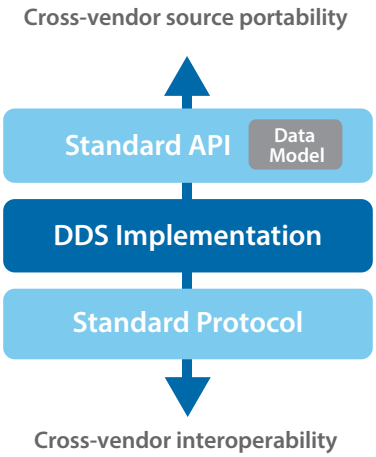

Figure 2. DDS standard

INTEGRATION OF EXISTING COMPONENTS

A DDS implementation, such as RTI Connext® DDS, is provided as a library. Each component of an application or system can be written or updated to incorporate DDS. This promotes a decentralized approach with low latencies and no single point of failure.

RTI also provides a DDS Routing Service to protect existing investments. (Fig. 3.) By building an adapter using an included software development kit, existing and unmodified applications or subsystems can be integrated into a DDS environment. This makes it easy to introduce DDS into any systems, and still allow peer-to-peer communication among all components.

To maximize connectivity, DDS can run on any device or system, ranging from embedded systems and mobile devices to cloud services. Data can be shared seamlessly across applications that are geographically distributed anywhere in the world. The protocol supports many programming languages and is supported on all popular operating systems and platforms.

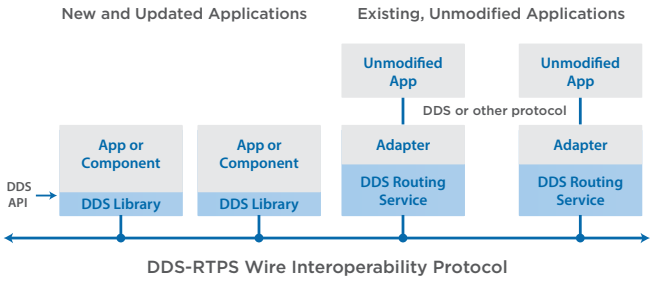

Figure 3. New and existing (unmodified) applications can co-exist on a Connext DDS DataBus.

SIMPLE AND RELIABLE PUBLISH AND SUBSCRIBE

On a DDS DataBus, components can rapidly and reliably share data. (Fig. 4.) For mission-critical industrial control systems, this provides many benefits:

- Simple, loose coupling. Adding a new sensor or actuator requires no changes to the other components and subsystems.
- Autonomous operation. Discovery is automatic, without a broker or centralized service.
- Non-stop availability. The decentralized approach avoids single points of failure.
- Visibility and control. QoS capabilities support real-time environments, and the DataBus provides status monitoring of system and component health.
- Flexibility. The DDS API is designed for embedded and enterprise systems, and the wire protocol also accommodates varying connectivity requirements.
- Low risk. Hundreds of thousands of devices successfully employ DDS today.

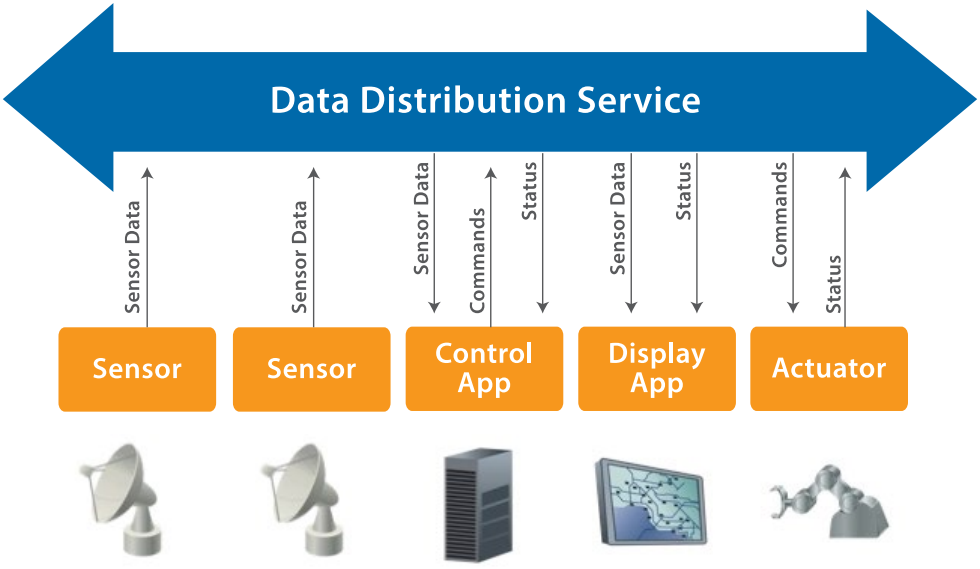

Figure 4. Publish and subscribe foundations of DDS.

DDS SECURITY

In March 2014, OMG published security extensions to the DDS standard. (Fig. 5.) Security capabilities are provided via plug-ins and require minimal or no change to existing DDS applications. Communication can be secured over any transport, including low-bandwidth and unreliable networks. Secure DDS does not require TCP or IP, and supports multicast for scalability and low latency.

The plug-in architecture, with built-in defaults, enables customizable security to suit unique requirements and take advantage of security-enabled hardware and firmware. Just like the foundational DDS features, the extensions support a completely decentralized architecture for high-performance and scalable control systems with no single point of failure.

An out-of-the-box implementation of these five security extensions (Table 1) supports common security algorithms for authentication and cryptography, and also supports fine-grained access control over which data users or devices are allowed to publish and subscribe.

For encryption, DDS provides control over which data and metadata must be encrypted and/or signed for authenticity and non-repudiation. It uses a hash-based message authentication code (HMAC). Encryption policies can be optimized for each data flow, making it possible to restrict security overhead appropriately and balance security requirements against any impacts on performance. DDS security is well suited for time-critical control systems and CPU-limited devices.

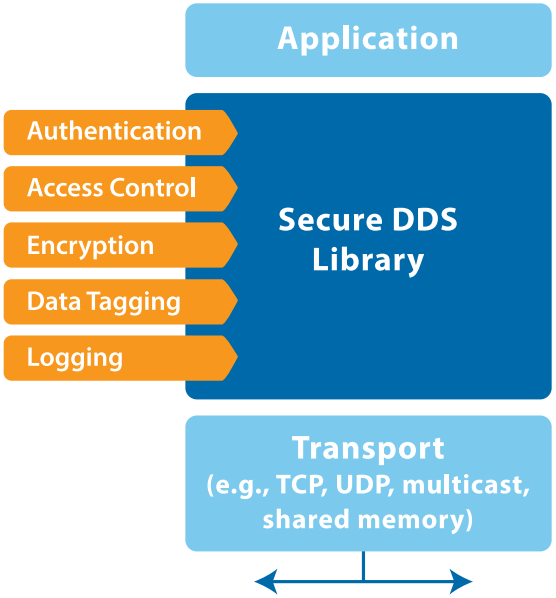

Figure 5. DDS security extensions

Authentication	• X.509 Public Key Infrastructure (PKI) with a pre-configured shared Certificate Authority (CA) • Digital Signature Algorithm (DSA) with Diffie-Hellman and RSA for authentication and key exchange
Access Control	• Specified via permissions file signed by shared CA • Control over ability to join systems, read or write data topics
Cryptography	• Protected key distribution • AES128 and AES256 for encryption • HMAC-SHA1 and HMAC-SHA256 for for message authentication and integrity
Data Tagging	• Tags specify security metadata, such as classification level • Can be used to determine access privledges (via plugin)
Logging	• Log security events to a file or distribute securely over Connext DDS

Table 1. DDS Security Extensions – Five Plug-Ins.

USE CASE: THE POWER GRID

In partnership with RTI, Pacific Northwest National Laboratory (PNNL) has applied the DDS security standard to secure an electric grid. Table 2 summarizes the security requirements, which were analyzed and addressed within the scope of a specific control station. DDS allowed a unique set of security policies to be introduced for each type of data flow.

Existing equipment and applications used the DNP3 protocol for connectivity, which has been well documented in terms of security problems. Using a retrofit approach, secure DDS connections were added between the control station and the transmission substation. (Fig. 6.)

The DDS Routing Service made it possible to introduce this connection without changing the existing DNP3-based devices and applications. DDS publish-subscribe capabilities allowed the insertion of new surveillance applications to non-intrusively monitor device status to detect anomalous activity and attacks.

DATA ITEM	AUTHENTICATION	ACCESS CONTROL	INTEGRITY	NON-REPUDIATION	CONFIDENTIALITY
Contol Traffic	X	X	X	X	X
Data Telemetry Traffic	X		X		
Physical Security Data	X	X			X
Engineering Maintenance	X				

Table 2. Security Requirements for Each Data Flow.

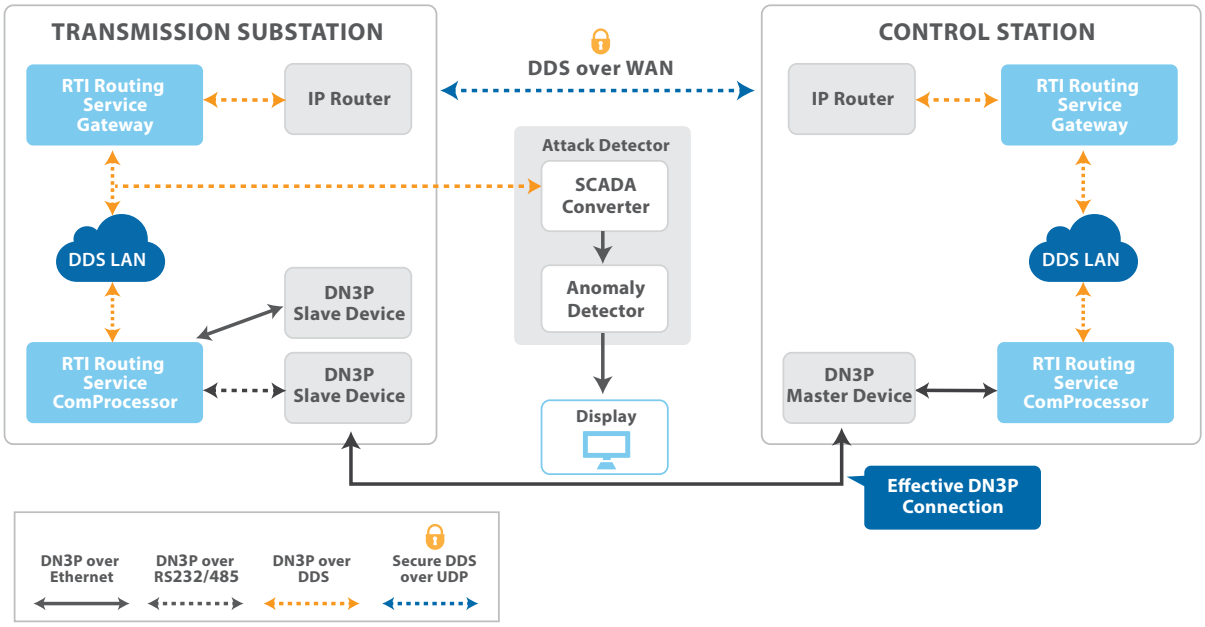

Figure 6. Retrofitting the power grid for boosted security and threat detection.

TO LEARN MORE

RTI Connext DDS, the leading DDS implementation, is at the forefront of the Industrial Internet revolution.

For more information about RTI Connext DDS and how to design smarter and more secure control systems, please visit www.rti.com.

You can also download a free trial of the RTI Connext DDS Solution.

ABOUT RTI

Real-Time Innovations (RTI) is the largest software framework provider for smart machines and real-world systems. The company's RTI Connext® product enables intelligent architecture by sharing information in real time, making large applications work together as one.

With over 1,500 deployments, RTI software runs the largest power plants in North America, connects perception to control in vehicles, coordinates combat management on US Navy ships, drives a new generation of medical robotics, controls hyperloop and flying cars, and provides 24/7 medical intelligence for hospital patients and emergency victims.

RTI is the best in the world at connecting intelligent, distributed systems. These systems improve medical care, make our roads safer, improve energy use, and protect our freedom.

RTI is the leading vendor of products compliant with the Object Management Group® (OMG) Data Distribution Service™ (DDS) standard. RTI is privately held and headquartered in Sunnyvale, California with regional headquarters in Spain and Singapore.

Download a free 30-day trial of the latest, fully-functional Connext DDS software today: https://www.rti.com/downloads.

Your systems. Working as one.

CORPORATE HEADQUARTERS
232 E. Java Drive, Sunnyvale, CA 94089
Telephone: +1 (408) 990-7400
Fax: +1 (408) 990-7402
info@rti.com

rti.com
rti_software
rtisoftware
company/rti
connextpodcast
rti_software