CAPABILITY BRIEF

RTI Connext: Securing Connected Medical Devices

A ZERO-TRUST SOFTWARE FRAMEWORK THAT ALIGNS WITH FDA CYBERSECURITY GUIDANCE

HIGHLIGHTS

Data-centric, zero-trust connectivity framework that protects data from unauthorized access across connected medical systems

Real-time, resilient and recoverable data communications across connected devices and distributed systems

Fine-grained security at both system and network transport boundaries, with configurable access control to protect data in motion

Modular and scalable architecture framework with no single point of failure

Compliant with the DDS-SECURITY™ specification and aligned with FDA cybersecurity guidance

The world's leading medical technology manufacturers rely on RTI for secure, real-time data sharing across distributed applications, devices and networks. RTI Connext® is a standards-based, proven software framework for securing communication interfaces, independent of network location or transport. It enables zero-trust security for data in motion to support next-generation surgical and connected digital healthcare solutions.

ALIGNING WITH REGULATORY CYBERSECURITY REQUIREMENTS

Protecting medical technology from unauthorized access is more critical than ever. Today's medical technology systems must be "secure by design." Device manufacturers must incorporate cybersecurity into their product lifecycle to ensure safety and effectiveness, and as a mandatory step in achieving regulatory approval. For instance, the U.S. Food and Drug Administration (FDA) will now issue "refuse to accept" (RTA) decisions for premarket submissions that do not demonstrate alignment with cybersecurity requirements. These guidelines include:

1. A definition of a security architecture that incorporates cybersecurity risks and controls throughout the design and implementation of the system and across all communication interfaces.

2. The implementation of security objectives (authentication/integrity, authorization, availability, confidentiality, and updateability) throughout the system architecture.

3. A secure product development framework (SPDF) that encompasses all aspects of a product's lifecycle, and mitigates cybersecurity risk as connectivity-based features are added.

As a trusted partner to many of the world's leading medical technology providers, RTI can help. Connext offers a software communication framework that is designed for low-latency, highly scalable and safety-critical systems. RTI provides state-of-the-art technology, software productivity tools, world-class services and support that powers next-generation medical applications and systems. Moreover, RTI's Long-Term Support (LTS) releases provide production-ready platforms to support a product's roadmap over the course of its lifecycle.

SECURE BY DESIGN

Industry best practices call for medtech manufacturers to perform threat modeling in order to comprehensively assess cybersecurity risks, and the corresponding design and mitigations to be implemented in order to protect the system. How do you ensure that connected healthcare applications and devices can be secure by design?

Least Privilege Access Control To Data In Motion

Connext enables "least privilege" access to data in motion, independent of transport or network location. Because the communication framework is "data-aware" by design, known data structures are only shared with authorized applications that need the data. This data-centric and decentralized architecture

requires no central brokers and provides data isolation-enabling features for flexible, secure and reliable architecture.

Zero Trust Design For Security, Reliability And Performance

Connext enables fine-grained configurability of security controls to be applied to data in motion. Built-in control plug-ins include authentication, cryptography, access control, data tagging and security logging to create a "zero trust" environment. Zero trust starts with identity as the new perimeter. Connext identity is based on PKI/certificate infrastructure, the industry's strongest type of identity. "Deny-by-default" permissions may be established based on the data and use case, and optimized for system performance across internal and external communication interfaces (Figure 1).

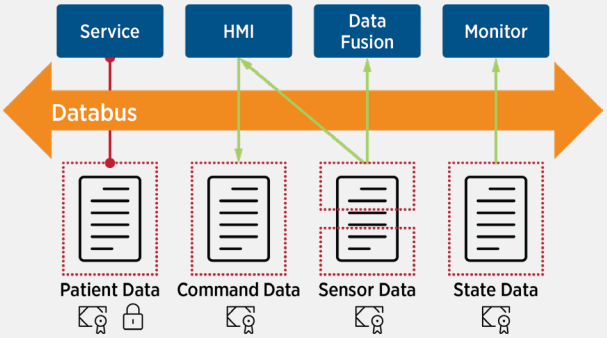

Figure 1: Data-centric cybersecurity provides the ability to design systems that restrict access control (e.g., authentication, encryption) for data in motion based on least privilege

The need for this level of control is essential to incorporate cybersecurity considerations for complex data sharing across interfaces and interoperable functionality — and is specifically called out in the latest, finalized **FDA premarket guidance.**

The inherently decentralized architecture of the Connext framework — along with extensive Quality of Service (QoS) features for reliable communications — help to ensure the availability of data access across connected systems, enabling resilient and recoverable dataflows.

Flexibility For Secure Development Life Cycles

Connext simplifies the configuration of advanced security controls and enables scalable security architectures as product features and integration requirements evolve. The configuration of specific controls requires little or no change to existing application code.

Secure Product Development Framework

The FDA guidance for premarket cybersecurity provides recommendations for device manufactures to demonstrate a secure product development framework. This includes consideration and detailed documentation of an end-to-end security architecture and the use of threat modeling to identify potential exploits across security domains, interfaces, and communication paths. Risks and mitigations must be considered across the device ecosystem and according to the use case. In addition, vulnerabilities must be managed post-market throughout the product lifecycle.

RTI offers products and services that map into the secure product development framework described in the FDA in the premarket cybersecurity guidance. RTI Professional Services Engineers can assist customers who are working to achieve FDA-related SPDF objectives such as Security Risk Management, Security Architectures, and Vulnerability Management.

FDA Cybersecurity Control Recommendations

The FDA defines specific guidance for various Security Control Categories. To meet these requirements, Connext delivers many technical features that support fine-grained security control down to the data model, to help users achieve FDA compliance. For a high-level mapping of regulatory guidance on Security Control Categories, please read the **Navigating FDA Regulatory Guidance** datasheet.

As cyber crimes become more sophisticated and the attack surface of complex and connected devices continues to grow, manufacturers need to stay ahead of the risks. Choosing a software communication framework that protects data in motion across applications, devices, and systems is a critical step. For more information on how RTI Connext can protect your system, contact us at **www.rti.com**.

Best-Practice Approach to Security

Today's best practices state that one should act as if the adversary has control of the network. How does a system operate securely in an environment that is compromised by definition?

The Answer:

Start from the principle of Zero Trust and assume dataflow must be protected at a granular level.

ABOUT RTI

Real-Time Innovations (RTI) is the infrastructure software company for smart-world systems. Across industries, RTI Connext® is the leading software framework for intelligent distributed systems. RTI runs a smarter world.

RTI is the market leader in products compliant with the Data Distribution Service (DDS™) standard. RTI is privately held and headquartered in Silicon Valley with regional offices in Colorado, Spain, and Singapore.

Your systems. Working as one.

CORPORATE HEADQUARTERS

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

rti.com
rti_software
rtisoftware
company/rti
rti.com/blog
connextpodcast