Top 10 Data Requirements for PDC

PAN-DOMAIN CAPABILITIES

Rapid changes in the global security environment are challenging militaries worldwide to seize, maintain, and protect their information and decision advantage over potential adversaries. These challenges require a focused effort to modernize how the joint forces develop, implement, and manage their command and control (C2) capabilities to prevail in all operational domains, across echelons, and with coalition mission partners. The Pan-Domain Capabilities (PDC) approach provides a coherent path for shaping future C2 capabilities. PDC is intended to produce the warfighting capability to sense, make sense, and act at all levels and phases of war, across all domains, and with designated partners, to deliver a decisive information advantage to the operational and tactical commander so they can converge joint and multi-domain effects at the speed of relevance.

This problem space is complex and is hampered by the current patchwork of brittle, stove-piped legacy systems, equipment, bespoke networks that support singular security domains, and a variety of data configurations with hard-coded, proprietary interfaces and structures that require data unpacking, translation, and repackaging at the tactical edge. This approach incurs significant overhead that throttles real-time networks and impedes the speed of convergence — at a time when real-time information delivery is paramount and can mean the difference between success or failure.

To drive increasing competitiveness, the U.S. Department of Defense (DoD), for example, has adopted a Data Strategy that states, "The DoD is a data-centric organization that uses data at speed and scale for operational advantage and increased efficiency." Furthermore, it mandates that, "It is the responsibility of all DoD leaders to treat data as a weapon system and manage, secure, and use data for operational effect."[1]

Created to accelerate the implementation of agile, highly-responsive systems, the PDC initiatives enable joint forces to implement service-specific solutions to address these network and interoperability needs. The implementation of these systems is now driving the emergence of data requirements that will guide and refine successful implementations of PDC systems.

PDC Data Requirements:

1. DATA CENTRICITY
2. NETWORK TRANSPORT-AGNOSTIC
3. MULTI-DOMAIN SECURITY ARCHITECTURE
4. ZERO TRUST / SECURITY
5. MODULAR OPEN SYSTEMS APPROACH (MOSA) AND OPEN STANDARDS
6. CLOUD TO TACTICAL EDGE CONNECTIVITY AND ENABLEMENT
7. DESIGN FOR DISCONNECTED OPERATIONS WITH DATA PERSISTENCE
8. INTEROPERABILITY
9. SCALABILITY
10. NETWORK HEALTH TOOLS

1. DATA CENTRICITY

To enable decision dominance at the speed of war, PDC systems must provide data to decision makers and decision-making Artificial Intelligence (AI) and Machine Learning (ML) systems across different operational commands, from the tactical edge to the cloud. This aligns precisely with the U.S. DoD Data Strategy announced on September 30, 2020 that directs DoD leaders to evolve all DoD assets into data-centric assets that treat data as a weapon system. This document outlines seven goals of this strategy — to make data Visible, Accessible, Understandable, Linked, Trustworthy, Interoperable and Secure (VAULTIS).

Data centricity refers to a system architecture where data is the primary and permanent asset, and applications come and go. Instead of exchanging messages, software components communicate via shared data objects that appear to be local data. Applications directly read and write the value of these objects, which are cached in each participant.

To reap the rewards to a data-centric architecture network, architects need to:

- Establish metadata tagging criteria
- Adopt and use standardized data interfaces
- Implement common data availability and access practices
- Incorporate data security best practices
- Establish PDC-conformant Information Technology (IT) standards
- Apply VAULTIS goals throughout the enterprise

The requirements for effective data integration must be considered from the earliest stages of data sharing and security and applied across the warfighting domains, in order to deliver rapid collection, fusion and customization of data.

Ideal for PDC systems, RTI Connext® is the leading software connectivity framework for implementing data-centric architectures in next-generation defense systems. It is built upon a peer-to-peer, data-centric architecture that delivers critical real-time data to AI and ML at wire speed, without servers or brokers. Connext is loosely coupled with a network discovery capability, enabling a network component “plug-n-play” capability. This allows users to dynamically insert new capabilities into a network that can be automatically discovered by operations technology, without powering down their systems.

The Connext architecture supports VAULTIS by design. Its application programming interfaces (APIs) drive access and visibility across multiple hardware and operating systems platforms in a consistent, understandable format. Its Real-Time Publish-Subscribe (RTPS) wire protocol drives rapid and consistent interoperability, while its open security capabilities enable trusted access across multiple security domains in real time. Connext enables a clear, open standards-based migration from network-centric systems to powerful data-centric environments, in many cases using the same network equipment.

2. NETWORK TRANSPORT-AGNOSTIC

PDC networks must support all network transports, as these include a multitude of physical links such as HF, V/UHF communications links, SATCOM, landline and/or optical fiber. Therefore, it is necessary to move data across wide-area networks to the tactical edge across all of these possible links in the path, without loss of data integrity. In addition, the PDC networks must eliminate the barriers between training and warfighting to enable a ‘train as you fight’ paradigm. The opportunities for Blended Synthetic [training] Environments comprising multiple actors in the air, on the ground or at sea are limitless with a properly instituted multi-domain network.

Connext works across all network transports, including UDP, TCP, InfiniBand, shared memory, and more. Connext naturally extends this connectivity to soldier training systems. This approach enables a migration from vendor-locked, server-based legacy training environments using HLA, DIS, CIGI and TENA standards to modern open gaming systems using Unity® and Epic Games® Unreal Engine®. Connext provides all training systems with access to live, real-time data from any field of operations. This enables very rich platforms that allow soldiers to train as they fight and use the exact data they will use in the fight. Connext is the ideal connectivity foundation for next-generation training systems, such as the U.S. Army Synthetic Training Environment (STE).

3. MULTI-DOMAIN SECURITY ARCHITECTURE

The PDC challenge is to support multi-domain operations (MDO) where the data from each network domain can be securely shared by multiple armed services, multiple defense supplier systems and coalition partners. Our global militaries currently have thousands of networks dedicated to a particular supplier, sensing system, weapon system or command and control (C2) platform. Each of these networks has its own security strategy and control of data in that domain, typically through a single-level, secure, dedicated network pipe. This network traditionally has trusted endpoints for data-in-motion and clear data from a single security domain inside the pipe, or full encryption of all contents in the pipe. Many of these systems use cross-domain platforms that are challenging to configure and cumbersome to modify to get data to mission partners.

RTI Connext enables an open and secure federated data fabric, so that operations data can be shared at the appropriate security echelon level.

4. ZERO TRUST / SECURITY

A Zero Trust environment assumes that adversaries are everywhere in the network. The network architecture must support securing data from all operational domains across the delivery environment. Individual data topics from each security domain need to be secured with unique data authentication and encryption strategies so only parties with appropriate credentials can access these topics. Multiple dedicated network pipes can no longer be a requirement. Instead, joint force C2 networks must employ layered security features supporting multiple military domains and be able to securely share data on optimized network pipes as permitted, enabling high network efficiency and lower operations costs. This entire environment must be free of single points of failure and must be standards-based for high scalability and rapid deployment by all domains.

RTI Connext® Secure, based on the open Object Management Group (OMG®) Data Distribution Service (DDS™) security standard, runs on top of working Connext systems, enabling the rapid inclusion of proven authentication, access control and cryptographic modules into mixed-domain, Zero Trust PDC networks. Connext Secure enables a standards-based security architecture that is independent of hardware and network platforms. Connext Secure is also ideal for securing data-in-motion deployments down to the level of individual data elements, with distinct security credentials on shared network pipes. This approach makes the need for dedicated networks for each security domain obsolete.

The capability to share operational data from different security domains can also enable the divestiture of networks with brittle, hard-to-advance characteristics, saving defense teams millions in costs.

5. MODULAR OPEN SYSTEMS APPROACH (MOSA) AND OPEN STANDARDS

All PDC future procurement should fully embrace MOSA and open industry standards. This would help the global forces to migrate from proprietary, stove-pipe solutions to an open systems architecture, fulfilling the 'system of systems' approach desired by all branches. Open standards also make global militaries less reliant on single vendors, opening the door to MOSA-compliant vendors and enhancing competition.

The PDC data fabric must incorporate efficient, evolvable and broadly applicable common data standards and architectures. To advance this concept, the global defense systems could adopt DDS as a foundation for building towards MDO capability. This can be done incrementally to mitigate risk and manage cash flow. The desired outcome is a multi-vendor, multi-domain capable network where data is seamlessly shared in an "all sensors, best shooter, the right C2 node" engagement paradigm.

Connext is based on the open DDS standard, which is managed by the OMG. It is used in defense networks and forms the connectivity foundation of over twenty MOSA standards, including FACE™, MOCU, Navy Open Architecture, OMS, ROS 2, SOSA™, TMSC, UMAA, UCS and more.

RTI is fully committed to open standards and was the first company to achieve FACE conformance certification for its Connext® TSS product that satisfies all requirements for the FACE Transport Services Segment (TSS).

6. CLOUD TO TACTICAL EDGE CONNECTIVITY AND ENABLEMENT

PDC networks must have enterprise cloud to tactical edge connectivity. Multiple combat cloud and tactical cloud technologies must be supported, including Google Protocol Buffers, Apache Kafka® and other legacy and emerging network strategies to enable instantaneous decision-making using the latest AI and ML. This architecture will drive:

- Enhanced shared situational awareness
- Synchronous and asynchronous global collaboration
- Strategic and operational joint planning
- Real-time global force visualization and management
- Predictive force readiness and logistics
- Real-time synchronization and integration of kinetic and non-kinetic joint and long-range precision fires
- Enhanced abilities to assess joint force and mission partner performance

Cloud enablement is relatively easy, due to the similarity of cloud systems. Far more challenging is enabling the tactical edge with similar capabilities using a diverse set of microprocessors and graphics processing units (GPUs) with the latest embedded AI and ML engines. Enabling tactical edge network systems with advanced, real-time decision-making available in cloud environments will deliver a consistent mission environment in the battlefield, even when networks are disconnected, congested and contested. RTI Connext drives real-time data connectivity from the cloud to the tactical edge using open standards-based technologies. Connext is loosely coupled and has a discovery mechanism to detect new capabilities, enabling a plug-and-play paradigm.

7. DESIGN FOR DISCONNECTED OPERATIONS WITH DATA PERSISTENCE

PDC networks will most certainly be under constant attack by adversaries across the entire communications chain. Therefore, global militaries must be able to operate with minimum guidance within a degraded or contested C2 environment, and commanders and staff must train aggressively in conditions where sensing and communications are severely impacted or completely disabled, and where adversary intentions are ambiguous. In addition, operations should be designed to be resilient to handle periods of limited bandwidth, disconnected devices and congested/contested network availability during critical operations. In addition, the Quality of Service (QoS) of data delivery must be designed to provide data persistence during periods of reduced data availability that can cause data denial for warfighters in the field.

RTI Connext has over twenty QoS settings to enable data persistence — its discovery capabilities allow the network to automatically heal and resume high-speed operations after network attacks, failures or loss of devices, nodes and systems. Connext enables secure access to data to the right warfighters during fully-connected, lossy, limited bandwidth and disconnected operations.

Connext enables a tactical edge-to-cloud environment that supports a common look and feel using shared data. In this manner, it can reduce training requirements for all warfighters in the chain of operations.

8. INTEROPERABILITY

The joint force data fabric must consist of efficient, evolvable and broadly applicable common data standards and architectures, with standardized key interfaces and services to access, aggregate, manage, store, process and share data across a large environment with a wide variety of partners and for operational uses. This wide range of mission participants demands rapid interoperability between disparate systems to bring to the fight the latest technologies and capabilities for the warfighter. The fastest and easiest way to do this is to have an open, standards-based wire protocol, so network applications can speak the same language.

RTI Connext supports the RTPS wire protocol, based on an open standard managed by OMG. RTPS in PDC systems guarantees interoperability between applications written in different programming languages and deployed on different systems by different defense suppliers. This enables a single, integrated coherent PDC network.

9. SCALABILITY

Universal and continuous information sharing must be designed and operated at the enterprise level. PDC applications and processes will depend on multiple enterprise nodes and supporting communications networks to provide global connectivity with the bandwidth, functionality and security needed to bring vital information to the joint force commanders. PDC systems must be able to rapidly scale to support diverse deployment designs and enable new operational units to 'join the fight' with existing networks, without loss of integrity. Joining units will need the same data model knowledge to properly interface with existing units. Note that since the network is 'equipment-agnostic' and adheres to MOSA and a common data model, the joining units can seamlessly tap into the PDC network — simply put, it is interoperability in action.

Connext delivers peer-to-peer architecture that eliminates dependencies on network servers and brokers, and is therefore able to provide secure data at physics speed between devices and warfighters. This has been proven in defense deployments, including sensor-to-shooter platforms with over ten million publish-subscribe pairs.

10. NETWORK HEALTH TOOLS

As stated earlier, PDC networks will be under constant attack by adversaries. Therefore, joint force C2 must employ a layered defense — spearheaded by a strong cyber defense — to deter malicious activity that would threaten enterprise operations. This cyber defense must have clear policy guidance, sufficient authorities, adequate training, timely intelligence and the technology necessary to conduct secure C2 in a globally contested environment.

Global militaries must adopt a wartime mindset during day-to-day operations — e.g., "train as we fight" — and develop knowledgeable leaders and staff with the training to employ the tools and authorities at their disposal. Merely deploying new networks with greater speeds and bandwidth will not mitigate these attacks or make our decision-making faster than adversaries. Tools will be required to determine network health, connectivity and availability.

RTI Connext Infrastructure Services enable developers to rapidly scale and integrate real-time, distributed systems based on a diverse set of technologies. Connext Infrastructure Services span a wide range of use cases, including Cloud Discovery Service, Web Integration Service, Database Integration Service, Routing Service and Persistence Service. These network health tools deliver unique and powerful functionalities that drive increased capabilities for any distributed system and help speed time to deployment.

In addition, RTI Monitor and Administration Console tools enable a consolidated perspective of cross-network operations for PDC networks, including detailed statistics on errors, traffic, resource usage, log analysis and system network topology display.

SUMMARY

These ten PDC network capabilities — Data Centricity, Network Transport-Agnostic, Multi-Domain Security Architecture, Zero Trust, MOSA, Open Standards, Cloud to Tactical Edge Connectivity, Design for Disconnected Operations with Data Persistence, Interoperability, Scalability and Network Health Tools — will enable a true Mission Partner Environment that is inclusive of all combined sensors, command and control. Optimized weapons systems across global militaries form the foundation of a successful, deployable and maintainable PDC environment.

RTI Connext, a commercial product, is already proven in defense networks and is the only technology that fulfills all of these demanding network requirements. Its existing deployment footprint vastly reduces the cost and time of realizing a viable and robust PDC environment. Connext peer-to-peer architecture eliminates servers and brokers, enabling real-time access to data at physics speed for all operations domains worldwide, as well as decision dominance at the speed of war. Connext is the ideal connectivity foundation for PDC, enabling a single unified network that can operate as one.

[1]Source - U.S. DoD Data Strategy:

ABOUT RTI

Real-Time Innovations (RTI) is the largest software framework company for autonomous systems. RTI Connext® is the world's leading architecture for developing intelligent distributed systems. Uniquely, Connext shares data directly, connecting AI algorithms to real-time networks of devices to build autonomous systems.

RTI is the best in the world at ensuring our customers' success in deploying production systems. With over 1,800 designs, RTI software runs over 250 autonomous vehicle programs, controls the largest power plants in North America, coordinates combat management on U.S. Navy ships, drives a new generation of medical robotics, enables flying cars, and provides 24/7 intelligence for hospital and emergency medicine. RTI runs a smarter world.

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 offices in Colorado, Spain and Singapore.

Download a free 30-day trial of the latest, fully-functional Connext software today: 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