Implementing Net-Centric Tactical Warfare Systems

Gordon Hunt

gordon.hunt@rti.com

Real-Time Innovations, Inc.

385 Moffett Park Drive, Sunnyvale, CA 94089

The tactical battlefield has long been characterized by the use of many different data collection and analysis systems that present information on small and discrete areas of the conflict to separate command and control stations. The operators of these stations attempt to use that data to estimate enemy intentions and actions, and counter with manual direction of the equipment and personnel in a simulacrum of coordinated response.

The result is a disjointed and often extremely dynamic environment of forces operating across the battlefield; a variety of aircraft with different weaponry, performance, and flight characteristics, fixed and mobile artillery, shipboard combat and weapon systems, and dismounted soldiers all with unique pieces of data when aggregated represent the complete strategic picture of the battlefield operations. However, these individual systems are typically focused on their individual missions, rather than on strategic coordination to achieve a larger objective. When these disparate systems are integrated, it is often with a particular mix and mission in mind. Each system is extremely capable and can win their individual battles, so to speak, yet lose the war due to a lack of coordinated activity. The advantage will go to the side that can keep up with the data and make it available where and when it is needed.

A much discussed way to dramatically improve the speed-of-command on the battlefield is to create a net-centric battlefield operation. Each individual element of a tactical system performs its narrow mission, but shares data as needed with others in a way that provides a more complete and accurate representation of the battlefield environment and the role of that system in the environment.

The purpose of net-centric warfare is to translate an information advantage into a battlefield advantage through the comprehensive networking and dynamic data-sharing between geographically dispersed forces. The shared situational awareness enables better strategic coordination of forces and enhances speed-of-command, which dramatically increases mission effectiveness.

But how is the net-centric vision currently being implemented? What is the design approach that enables the concept? How is this design approach being realized given that our start point is already deployed systems which were not originally architected to fit into a net-centric design?

Data-Centric Orientation Drives Net-Centricity

Net-centricity doesn't happen without a specific set of goals in mind. Defense planners and acquisition program managers have to determine that it is a necessary objective, determine what form it will take and mandate an open common communication architecture.

In the past, systems have been designed with point-to-point data communications that focus on delivering data from the sensor directly to an operator. In these cases, the endpoints are known to both producer and consumer, and the data format is agreed upon and unique. Modern 'distributed-systems' can readily be broken down into a collection of hard-wired static point-to-point communication links.

Point-to-point connections between individual systems are fragile, and certainly don't meet the requirement for dynamic-data integration between multiple systems. The correct approach is to provide real-time connectivity to all systems within the battlefield framework, move the limited intelligence and data away from the individual system and onto the network as a whole. Once the data is abstracted from the individual system and made available across the network, numerous applications can be written to analyze and act on it, providing a significantly higher level view and a faster response time.

Achieving a data-oriented perspective on the environment has proven to be critical to building the net-centric architecture. A focus on the data within a distributed-system is already enabling network and application designers to grasp the information opportunity.

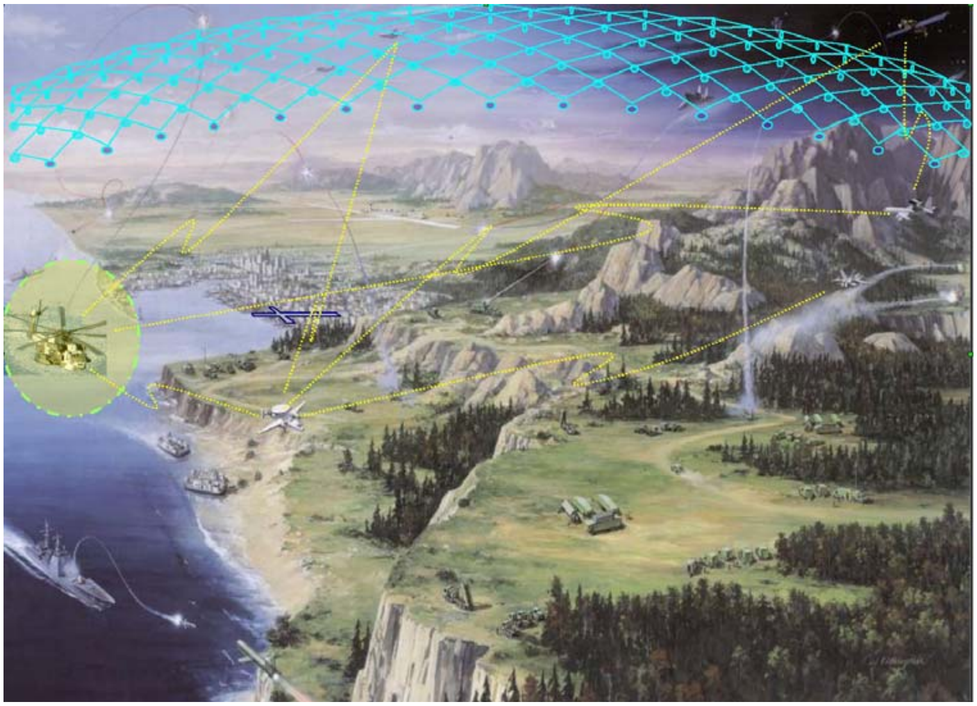

Figure 1: A Data Oriented Net-Centric Battlefield

The battlefield is an especially difficult network environment, with both signal interference and transient data sources a fact of life. With point-to-point connections, when a data source or connection is lost, the data consumer loses that information, even if it may be available elsewhere on the network. In a data-oriented environment, the data is resilient, in that it is abstracted away from the source. If there are multiple sources or connection options, data remains available as long as one source or connection remains active. By achieving this level of fault tolerance, the data-centric network remains highly operational even as data from individual sources degrades.

In the dynamic environment of the battlefield, the data sources will be transient as they enter the battle space. For example, feedback from a missile may only exist until it detonates, and only became relevant after its launch. A video feed from a UAV may only interesting to both the strategic commanders as well as the forces on the ground when the UAV if flying over a certain area. In these environments, applications that want to aggregate the data into useful information cannot know a-priori how to talk to every data source, what data sources will be present, nor when to attempt communication with data source it may know about. Data-oriented principles describe a method to expose your data into a global data space maintained by the network itself. The data becomes accessible to any application or system requiring it and is decoupled from the system state of the application producing it. Notification of the availability of required data occurs automatically through discovery mechanisms and the data itself drives the applications. In such an environment you do not need to know or care from whom the data originated, nor how it became available (transport mechanism), merely that it exists and is available for you to act upon.

The validity of this data-oriented architecture for net-centric system deployment has been proven time and again to be the OMG Data Distribution Service (DDS), built around an open-standards data-centric model. By using data-oriented concepts in analyzing the problem and implementing the solution on DDS, system designers have been able to create the composite elements of a net-centric battlefield.

Commercial off-the-shelf products that have implemented the OMG DDS standard have been used in a growing number of both new and existing weapons systems projects with great success. These systems are particularly adept at coordinating, analyzing, and responding to data across large-scale networks where response time is critical and resilience to battlefield events is mandatory.

A key enabler of the resilience in these systems is the rich set of DDS definitions of application level Quality of Service (QoS). Every producer and consumer of data to the global data space defines their service capabilities or requirements through a QoS contract broker, and DDS ensures there is a match before the communication is established. Even if the data is available, but the contract of service between producer and consumer is broken (such as when agreed data update rates are not being met), an alternative data supplier will be automatically sought by the DDS middleware to meet the required contract of data service. The DDS QoS captures all of the fault tolerance, stateful behavior, controlled access to data, and protocol issues which in the past have been handled on a per-system basis, and abstracts them for use in a dynamic net-centric environment.

Achieving Net-Centric Goals in a Battlefield Environment

Net-centricity through the use of data-enabled battlefield systems and a comprehensive data-distribution system is not merely a theory or abstraction. Weapons systems have been putting it into practice with new development efforts as well as existing system modification projects. As systems are conceived or upgraded over the course of their operational lives, they must be enhanced with hardware and software to expose their tactical data and make them a part of the distributed system whole.

An example of such a system enhancement is the Navy E2-C Hawkeye. The Hawkeye provides all-weather airborne early warning and command and control functions for the carrier battle group. Network and system upgrades for this venerable weapons system include the addition of middleware incorporating the tenets of data-centric design, performance optimization (especially latency and data throughput), portability across existing and future architectures, hardware and operating systems, as well as security best practices as defined by Common Criteria Information Assurance.

The original Hawkeye had a number of sensors and data collection devices, with a variety of one-to-one and one-to-many connections to other devices or to operators.

The goal of development effort was to provide a platform by which data from the many radar systems and sensors on board the Hawkeye platform can be aggregated together for analysis of signals to determine the extent of a threat, and to suggest action for neutralizing that threat. The focal point for this effort became the data integration and a conceptual data-bus (otherwise known as the global data space), rather than individual connections between devices and operators. By abstracting the data and the data's QoS away from the application layer and into its global data space, current systems as well as future enhancements can leverage the data not worrying about data source implementation details. This approach also enables any future enhancement efforts freedom to better use COTS hardware, and also enables engineers to make design decisions that are based on system objectives rather than on specific technologies. See Figures 2 and 3. The first shows the modular design with all the point to point connections that existed. The red lines indicate the new connections that needed to be added.

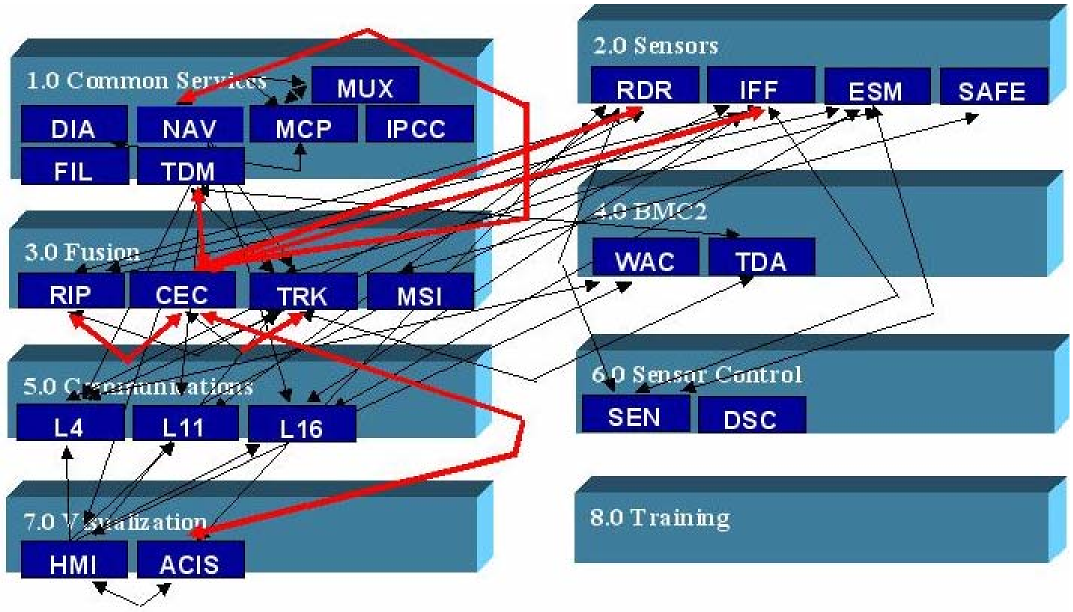

Figure 2 – The Hawkeye system design prior to adopting a data oriented communication model

The second figure shows how all of the connectivity complexity has been extracted away from the application and managed by the conceptual data bus.

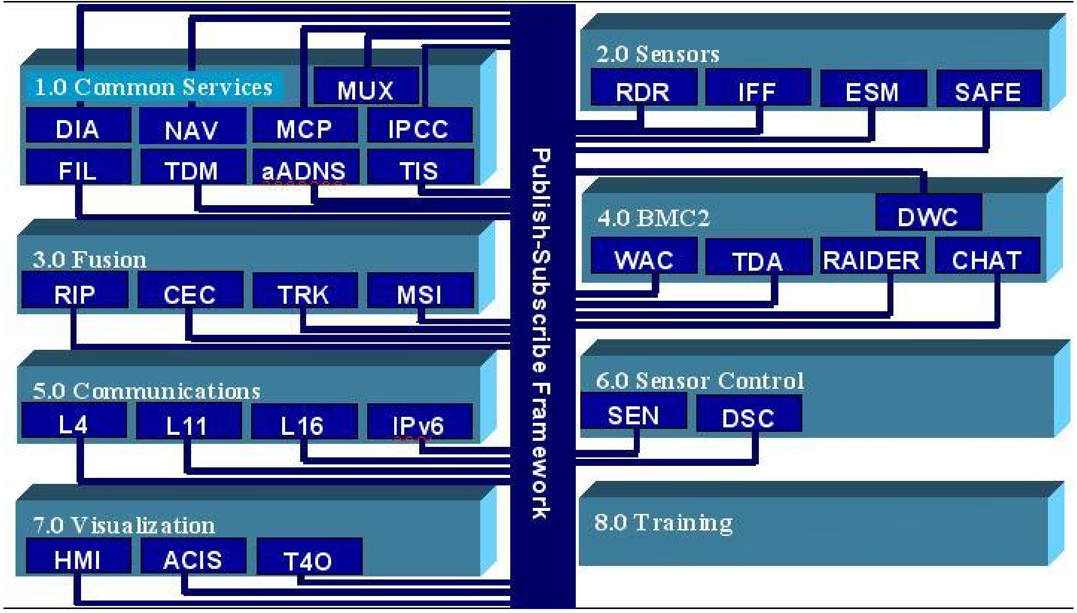

Figure 3: The Hawkeye Software design after DDS had been used to implement a data oriented communications model

A primary function of UxV's is the collection and communication of real-time battlefield information into the net-centric view. General Atomics Aeronautical Systems Inc is a renowned market leader with its' Predator, Predator B, Sky Warrior Alpha and Sky Warrior Block 0 UAVs. They have adopted a data oriented development model to enable a single Advanced Cockpit Control System to interface to the telemetry systems of all these UAVs. The cockpit includes a Common Operating Picture to assist the pilot in understanding the combat situation facilitating a higher level view of the battlefield than just a streamed video feed. See Figure 4

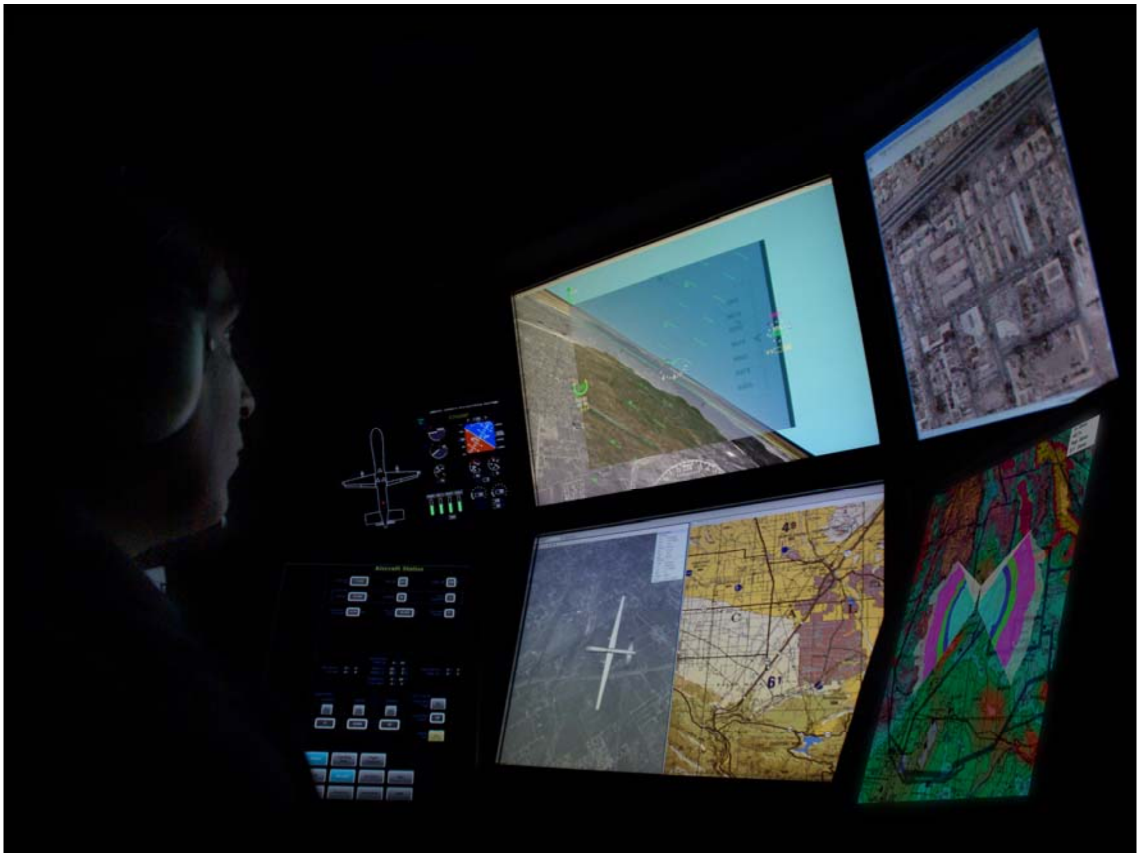

Figure 4: General Atomics Advanced Cockpit Control Station

In a similar manner, the Navy Open Architecture program is a foundation for the modernization of the Navy's cruisers and destroyers, including the Aegis upgrade, the Total Ship Computing Environment (TSCE) and the Littoral Combat Ship (LCS). The Open Architecture program incorporates Data Distribution Services that enable the on-time delivery of data across the network to the subscribing components, even if they change during the course of system upgrades and enhancements.

The Open Architecture program has been commonly implemented through network middleware that uses a publish-subscribe model for data. Such a model (OMG DDS) separates the data from its source and makes it accessible to any application running on the network; thus enabling the Open Architecture program to provide a data-centric environment that's amenable to expansion with new systems and applications.

The weapons systems utilizing the Open Architecture program are taking advantage of the flexibility inherent in its data-driven architecture to reduce the cost of those systems while making them more adaptable to different mission requirements. For example, the LCS derives combat capability from rapidly interchangeable mission modules and the open architecture command and control system.

Although connectivity using a data-centric orientation is a prerequisite, simple connectivity through network hardware and communications protocols doesn't suffice to deliver a net-centric weapon system. Two elements are missing. The first is a series of standards that guide systems development projects, and the second is a comprehensive distributed infrastructure upon which network applications can be hosted.

Standards Drive Net-Centricity

Standards play a key role in enabling data-driven net-centricity across all systems on a battlefield. Without standards, it will not be possible to coordinate the data being produced and consumed by the myriad of systems and devices on the battlefield. There must be some roadmap that helps to determine data format and throughput requirements in order to provide a common foundation for applications utilizing the network and acting upon the data.

Ultimately, the network infrastructure has to provide support for a net-centric approach to battlefield operations. Currently, incompatibilities exist between individual weapons systems with regard to characteristics such as protocols used, bandwidth, frequencies, and media. Without a common network infrastructure, systems will be unable to interoperate effectively.

A driving force behind the development of a common network infrastructure for the US Navy and Air Force is the Net-Centric Enterprise Solutions for Interoperability (NESI). NESI provides, for all phases of the development of net-centric solutions, guidance that meets DoD Network-Centric Warfare goals.

NESI implements higher-level defense directives, including the Net-Centric Operations and Warfare Reference Model (NCOW RM) and the ASD (NII) Net-Centric Checklist. NESI is a body of architectural and engineering knowledge that guides the design, implementation, maintenance, evolution, and use of the Information Technology portion of net-centric solutions for military application. NESI provides specific technical recommendations that can be used as references.

From a practical standpoint, NESI drives the abstraction of individual systems data to a common data-driven environment. It marks a step toward the use of a comprehensive data bus, similar to the Enterprise Service Bus (ESB used in the non-real-time SOA environment), that manages the flow of data between multiple weapons systems in a hard real-time networked environment. For example, a navigation system publishes navigational data to the bus, rather than hard-coded data intended for one specific use.

Consider navigation data onboard the littoral Combat Ship. There are numerous sensors that can provide information about the ships course and speed and certainly the combat system views this data as critical for its function. When deploying a combat system one could hardwire a particular navigational sensor into the combat system, coupling the two systems by defining data format, temporal delivery semantics, fault and failure conditions, source and destination addresses etc. Doing so makes the replacement of the navigational sensor a major software/hardware evolution. A data-centric approach mandates that the data (in this case nav-data) be described in an open format and all behavioral semantics regarding the data be described in the QoS, not buried in singular application logic. Thus, when replacing the navigation sensor one simply has to publish data according to the nav-data interface, all other combat system functions remain unchanged.

An Integrated Network Infrastructure

All of this leads to the infrastructure required for a fully net-centric battlefield. In such an environment, applications and application components such as Web services can be hosted on processing nodes and be able to access and use any data on the network. This requires the combination of media, protocols, and middleware to support full connectivity and data access anywhere on the network in real time.

According to the DCIO OSD Networks and Information Integration, such an infrastructure will make use of Internet Protocol Version 6 (IPv6). It will also provide for secure and available communications requiring trusted sharing of network resources, and one-time handling of information, posted by authoritative sources. Most important, data should be posted and made available as it is created, and applications on the network be written to encourage discovery of data when and where it is needed. And in order to ensure good application and network architecture, data is kept separate from applications.

Several efforts are underway to establish the infrastructure that meets these requirements for a battlefield network. In particular, because many battlefield systems already exist and are in active use, this infrastructure has to work to combine devices that were not originally meant to talk to one another. In fact, they may not have a data communication interface at all.

This presents a number of challenges to the building of a net-centric battlefield. One project that addresses this is the Common Link Integration Processing (CLIP) program. The CLIP program was implemented to develop common software and common-link processing for a joint Army-Navy-Air Force program. It allows existing platforms without a tactical data link, as well as platforms with different tactical data links, to communicate with each other. When CLIP is installed, these platforms can exchange information digitally without having to rely entirely on voice radio transmissions or hard-wired and independently configured tactical data links. CLIP consolidates these tactical data links and gives the military services the capability to share information across systems.

CLIP operates within multiple computing environments and data communication environments, complying with network-enterprise service-interoperability standards and the tactical radio system software communications architecture. The CLIP design framework includes a wideband networking platform, tactical targeting network technology, an enhanced position-location reporting system, an integrated bridge system, and joint range extension application protocol processing software. CLIP enables a data-centric orientation across the network so that middleware and applications can implement architectures that make data a first-class citizen, and thus DDS has become one of its building blocks. For example, CLIP combined with a DDS standards implementation can translate legacy data messages into a distributed services global data space, available for consumption by all systems on the network.

Fully leveraging this capability is the Boeing B-1B effort. By using CLIP with a data-centric DDS interface they can simply subscribe to “Tracks” and receive all track updates from numerous tactical data links without worry of data format, data state, failure semantics, or data source – the middleware and QoS based data-centric infrastructure manages these details.

Once CLIP and similar projects are completed and deployed, systems and devices on the battlefield will be able to link up and exchange data. These will not be one-to-one connections, but rather a true distributed network with data from one device able to be identified, received, and consumed by any data processing system on the network.

Toward a Comprehensive Battlefield Network

Despite these and other efforts, much work remains on the creation of a net-centric approach to battlefield operations. A big step in building out a data-driven network is the infrastructure for communication across the hundreds of different types of devices in a dirty and noisy environment. The infrastructure incorporates media, protocols, and middleware that enable performance and service characteristics across multiple connected systems and devices.

Separately, hundreds of different types of individual devices must be built or modified in order to connect to the distributed network and readily exchange data across that network. While many devices have data links that provide one-to-one connections and limited networking capability, a combination of modifications coupled with programs such as CLIP will gradually enable greater and more effective use of data in the net-centric battlefield view.

It also requires a change in the design process of new and modified weapons systems to publish data, rather than target a specific data consumer such as an operator. Over the lifetime of that system, the need for its data will grow and expand beyond its original single-point target. The point of integration on the network is the conceptual data bus (global data space), supported by distributed data services.

But beyond the network infrastructure and data communications among the multiple devices, applications using data-driven architectures must be built in order to take advantage of real-time data availability from multiple network nodes. These applications must have seamless access to data from multiple devices, reach a determination on a course of action for a single system, or a set of battlefield systems, and cause the execution of that course of action through a coordinated response of weapons systems or other battlefield devices.

It will take years for the vision of a true net-centric battlefield to emerge to reality. But the benefits will appear gradually, as the network and its components systems are built out and deployed in the field. Data-driven applications can be written today to give battlefield commanders greater insight into operations and force deployment.

To learn more about applying net-centric principles, visit www.rti.com.