

# SOSCOE—The Glue That Holds FCS Together

LTC Dave Bassett and David Emery

**I**n modern network-centric warfare, information is simply another aspect of combat power. A force's total fighting capability depends on its ability to fire, maneuver, gather and use intelligence, provide logistical support and gather information and apply it to command and control. The Army's Future Combat Systems (FCS) is largely about just that — information.

SOSCOE is the foundation for FCS-networked software for numerous Army systems, including the vehicle management systems for the Stryker. Here, a U.S. Army Soldier from C Company, 3rd Battalion, 21st Infantry Regiment, 1st Brigade, 25th Infantry Division (Stryker Brigade Combat Team), pulls guard while fellow Soldiers load into their Stryker in Mosul, Iraq. (U.S. Army photo by SPC Jory C. Randall, 55th Signal Company (Combat Camera).)

As the first Army system to be designed for network-centric operations, FCS is a leader in integrating new Global Information Grid (GIG) standards. However, the system also inter-operates with Current Forces, allowing the program to provide useful spin outs that benefit Current Forces.

Network capability for the FCS-equipped Unit of Action (UA) will be implemented as an integral part of the GIG and the Army's LandWarNet approach. The FCS program's network comprises several key components:

- Network standards
- Network transports
- Network services
- Applications
- Platforms
- Sensors

While building and deploying network transport, applications, platforms and sensors are well understood, this new architectural approach's network services layer has been more difficult to define. GIG descriptions separate services into core and application services. For FCS, these core services are implemented by a common set of open standards-based software components tailored to the safety-critical/mission-critical, real-time/near-real-time needs of the FCS family of systems (FoS), including both manned and unmanned platforms. These components are called the Systems-of-Systems Common Operating Environment (SOSCOE).

This article explores FCS SOSCOE's role as the "glue" that ties the FCS FoS together as a critical FCS Net-Centric Information Environment (NCIE) component and SOSCOE's role in the

FCS approach to realizing DOD's "net-centric vision."

**What Is SOSCOE?**

SOSCOE is the foundation for FCS networked software including vehicle management systems; command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR); Soldier and unmanned air and ground systems. Just as an operating system on your computer allows you to interact with resources and other computers, SOSCOE al-

lows battlefield systems to communicate and interact with the UA. SOSCOE provides several key functions:

- Internal FCS information delivery and management mechanisms.
- Interoperability services.
- Data storage.
- Security and information assurance services.
- Information discovery services.
- Web services.

The FCS network approach's overarching goal is to allow commanders and their staffs to manage all information required to execute their mission. It is important to note, however, that the primary SOSCOE user is neither the commander nor the Soldier, at least not directly. Rather, SOSCOE delivers a reusable set of software components that platform integrators and application developers use as the foundational building blocks of their software code. This allows developers to focus on their code's "business logic" rather than dealing directly with the complexity of the tactical network environment (underlying tactical network transport environment).

In modern network-centric warfare, information is simply another aspect of combat power. ... The Army's Future Combat Systems is largely about just that — information.

The goal is for SOSCOE — not the application developer and certainly not the Soldier — to deal with the unique and complex tactical communications infrastructure in which FCS must operate on the battlefield.

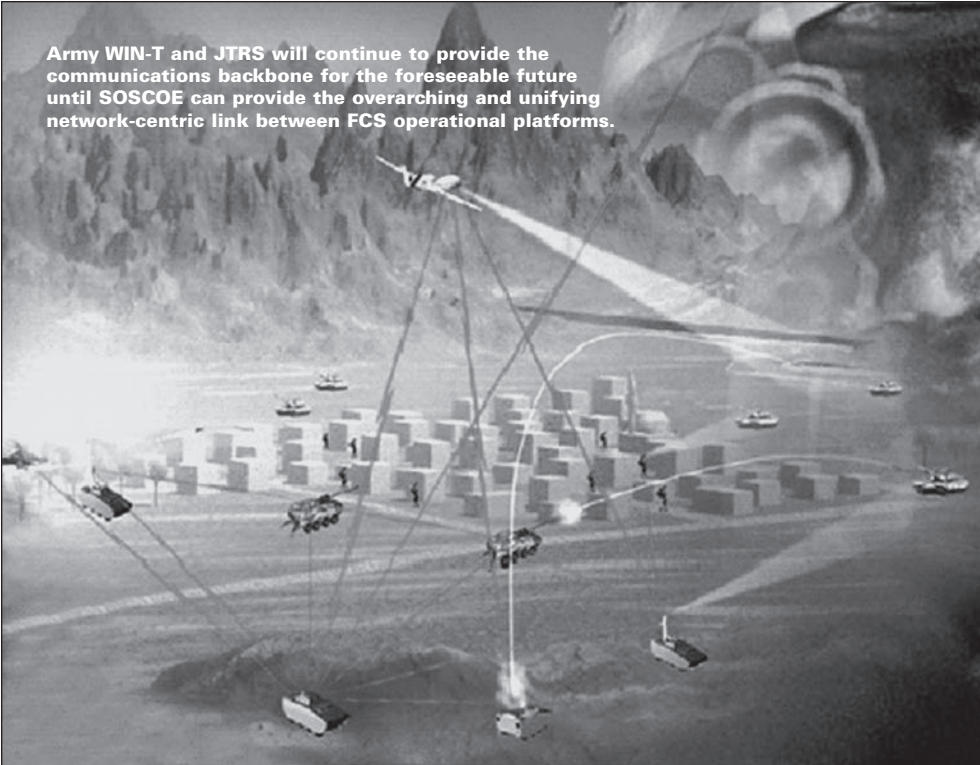
SOSCOE provides the common services of the NCIE, integrating information distribution within the UA and making FCS battle command services and data available to other Army and enterprise users throughout the GIG. The NCIE concept provides for seamless access to data throughout the GIG, regardless of where that data is located.

**NCIE**

NCIE encompasses the entire spectrum of hardware and software C4ISR systems used to manage and disseminate information to, from and within the UA. The NCIE's mission is to provide the right information to the right warfighter at the right time, in the right medium, the right language and at the right level of detail. Other NCIE parts include:

- Joint Tactical Radio System (JTRS) Cluster 1, Cluster 5, network data link (NDL) and Warfighter Information Network-Tactical (WIN-T) communications networks monitored and managed as a shared communications backbone.
- A network management system capable of integrating and dynamically managing the bandwidth of the JTRS, WIN-T and NDL communications "pipes" into a single, adaptable logical network. The network must integrate with the FCS platform, including the FCS network management system and services.
- Battlefield sensors to provide information on the UA's status — including logistics sensors and Blue Force Tracking information — and the enemy. The sensors are "network

Army WIN-T and JTRS will continue to provide the communications backbone for the foreseeable future until SOSCOE can provide the overarching and unifying network-centric link between FCS operational platforms.



aware,” making information available to the UA as well as to the larger set of GIG subscribers.

- FCS battle command services that fuse sensor information with planning data and human inputs, producing an information environment focused on meeting the commanders’ needs and providing automated and semiautomated decision support.
- A unified, GIG-compliant, data model referred to as the “FCS One Model.” Metadata is ubiquitous across this model in compliance with GIG requirements.

While bandwidth within the bounds of each FCS platform is abundant, it is the JTRS and Army WIN-T communications backbone that brings the platforms together into a unified net-centric force and links that force into the GIG communications backbone. These radio networks provide far less bandwidth than the internal hard-wired networks. Rather than providing battle command services and situational awareness to only a fraction of the UA platforms (specifically equipped with

direct connectivity to high-bandwidth satellite communications), the FCS network approach extends connectivity and corresponding network capability down to each platform and Soldier.

A consequence of bringing more users into the net-centric environment is an increased density of subscribers sharing the UA’s communications system. It is clear that exposing all UA subscribers directly to the Net-Centric Enterprise Services (NCES) would significantly exceed available bandwidth.

The ability to seamlessly cross boundaries on the network from UA to Unit of Employment and beyond necessitates carefully managing scarce resources to ensure that those resources are applied with the proper priorities, thus providing maximum benefit to warfighters. The FCS NCES portfolio proposal will address the need to manage services use across the boundary between the UA and higher echelons.

### Net-Centric Design

SOSCOE is only part of the overall

NCIE in the FCS-equipped UA. The FCS design increases the warfighter’s awareness of and access to information, maximizes the ability of the underlying communications networks (JTRS, WIN-T and NDL) to deliver that information and enhances the UA commander’s ability to control and prioritize information dissemination within the area of responsibility.

DOD has chartered a Program of Record for NCES to provide implementations of GIG core services to the DOD Enterprise. The communities of interest (COIs) define domain-specific services that will leverage the underlying NCES core services. The specific set of potential core enterprise services are: enterprise systems management, messaging, discovery, mediation, collaboration, user assistant, information assurance (IA) and security, storage and applications that allow plug-in of COI capabilities.

The NCES program does not provide data transport. Rather, NCES is dependent upon adequate bandwidth and GIG infrastructure availability, relying on GIG transport services and tactical communications systems for all data exchange. It is clear that — given the lack of bandwidth-oriented metrics supporting the NCES Analysis of Alternatives and in discussions with the office of the Secretary of Defense’s Network and Information Integration Office and others — the initial NCES increment services will be focused on meeting the needs and bandwidth availability of strategic, rather than tactical, systems.

FCS implements net-centric concepts both within the architecture of each combat platform as well as in the C4ISR architecture that brings the various platforms together into the integrated UA. Specific design tenets directly addressed include:

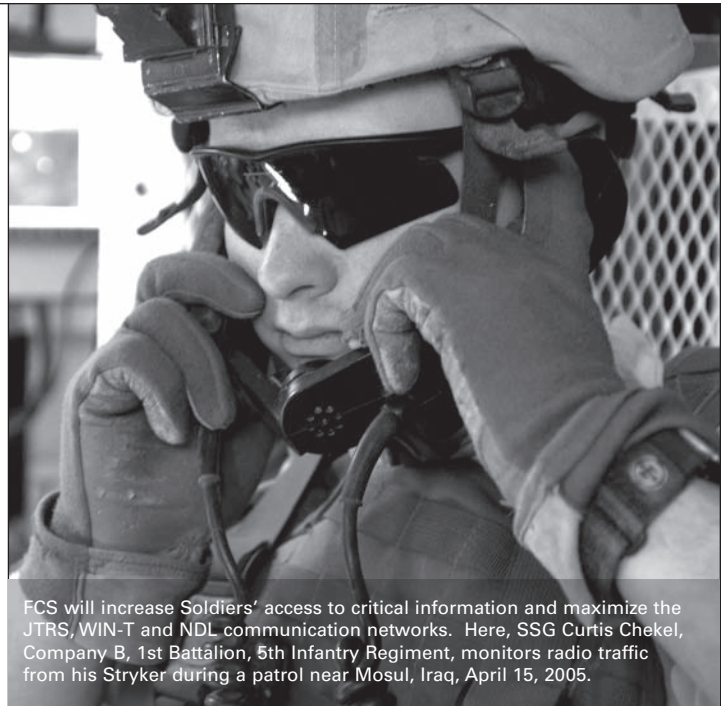
- **Make data visible.** All data within the FCS UA system is published to the FCS NCIE and will be published to NCES-based systems to the maximum extent bandwidth allows. This mechanism is “soft-wired” into the system through policy and metadata interpreted by the SOSCOE. While bandwidth will not be sufficient to make all FCS data visible to the enterprise, the FCS NCES effort will maximize data visibility to NCES services.
- **Make data accessible.** The FCS NCES-managed connectors will make data and services accessible per the standards and mechanisms required by the core enterprise services, service discovery and content discovery services. All data will be metadata tagged and marked for security classification to maximize coalition accessibility.
- **Make data trustable.** Role-based access control and NCES IA services integration will result in trustable data across the UA and up to the enterprise.
- **Provide data management.** The density of users and sensors in the UA results in substantial amounts of data. SOSCOE data-store services — both local and distributed — provide data management to user applications in a standard, open way across the FoS.
- **Open architecture.** The entire FCS software architecture is based on layered, open architecture and open standards. All Web services provided by SOSCOE use the latest industry standards of hypertext transfer protocol, hypertext markup language, transport control protocol/Internet protocol, extensible markup language, cascading style sheets, simple object access protocol and the Commercial Joint Mapping Toolkit.
- **Identify management and authentication.** Information assurance services integrate role-based access controls across the communications and data store middleware. The net-centric connector that FCS NCES will

provide will link these services directly to the NCES security services in a managed way across the bandwidth-constrained boundary.

The special challenge for FCS is to provide seamless network access over an ad-hoc, mobile, limited-bandwidth network. Unlike many other ad-hoc networks, such as a public cell phone system, the absence of fixed centralized nodes in the FCS network further complicates the design. By building on SOSCOE, combat platforms — from Soldier hand-helds to sensor networks to manned command and control vehicles — provide and obtain information that integrates into a UA-wide managed information network.

Thus, the FCS challenge is to integrate seamlessly with NCES and GIG high-bandwidth transports, while managing the reachback from the UA into NCES and, more importantly, the *reachforward* from NCES into the UA’s tactical NCIE. In general:

- FCS will employ tailored SOSCOE discovery and dissemination within the UA and between tactical systems employing SOSCOE or SOSCOE-compatible services.
- FCS will expose data and services in NCES-compliant standards where the network environment supports those standards and protocols, primarily coincident with WIN-T points of presence providing nonterrestrial, high-bandwidth communications linkages to GIG transport.



FCS will increase Soldiers’ access to critical information and maximize the JTRS, WIN-T and NDJ communication networks. Here, SSG Curtis Chekel, Company B, 1st Battalion, 5th Infantry Regiment, monitors radio traffic from his Stryker during a patrol near Mosul, Iraq, April 15, 2005.

SOSCOE provides for net-centric information “enclaves” at the tactical level, allowing for all elements within the UA to participate in the overall GIG environment.

As DOD evolves toward a fully net-centric DOD, FCS is the system that implements the last tactical mile of the Army’s LandWarNet architecture and extends the GIG directly into the hands of American Soldiers.

---

LTC DAVE BASSETT is the Product Manager (PM) for UA Software Integration including the FCS SOSCOE. He also serves as the government’s Chief Software Engineer for the FCS C4ISR Integrated Product Team. He holds a B.S. in electrical engineering and an M.S. in computer science, both from the University of Virginia.

DAVID EMERY is Chief Engineer for the PM UA Software Integration and Chief Software Architect for DSCI Inc. He holds a B.S. in mathematics from Norwich University and is a retired field artillery and automation officer.