ARCHITECTURE FOR A

TRULY INTEGRATED DEFENSE NETWORK

Eric C. Firkin,
Solipsys Corporation
Laurel, MD 20707
eric.firkin@solipsys.com

Margaret M. McMahon, Ph. D.
Computer Science Department, US Naval Academy
Annapolis, MD
mmmcmahn@usna.edu

Architecture for a Truly Integrated Defense Network

Eric C. Firkin,
Solipsys Corporation
Laurel, MD 20707
eric.firkin@solipsys.com

Margaret M. McMahon, Ph. D.
Computer Science Department, US Naval Academy
Annapolis, MD
mmmcmahn@usna.edu

Abstract

The National Capital Region (NCR) of the United States of America (U.S.) is a microcosm of all that is difficult in creating a regional, integrated defense against terrorism: multiple civil jurisdictions, target-rich environment, and the requirement to involve many organizations in any decision. The Region's current defense lacks a truly Integrated Defense System (IDS). Through the use of a demonstrated and available Network-Centric Warfare (NCW) solution, there can be significant improvement in the timeline and quality of decision makers' response to threats.

Regional radar systems have an effective data path to military fighter aircraft and missile batteries in the NCR; however, there are other governmental, non-military systems generating data that could also contribute to the real-time picture. This non-military data cannot always flow to decision makers, and when it does, inconsistencies between the disparate systems require human input to resolve.

An NCW application would allow these stovepipe systems to share data, thus producing a common picture of the Region. The Tactical Component Network (TCN®) provides an architecture that is successfully deployed by the U.S. military today and can be implemented immediately. The more complete and common picture provided by TCN reduces the threat response timeline.

TCN Relevance to Command and Control

The events of September 11th, 2001 demonstrated weaknesses in the ability of the U.S. to defend its own borders. Many initiatives have been undertaken to answer some of the noted shortfalls but none has taken the final step required to develop and implement a fully integrated network linking all levels of Command and Control (C2).

Systems such as the U.S. Army Air Defense Artillery (ADA), U.S. Air Force fighter aircraft, and U.S. Customs helicopters in the NCR receive aircraft flight data from the Federal Aviation Administration (FAA) radar network and U.S. Army Sentinel radars. Often there is no common machine-to-machine language linking these systems to facilitate seamless information sharing; each system must maintain its own vision of the defended area. This drives the length of the timeline required to respond to incidents and dramatically increases the opportunity for both system and human error.

TCN would provide command authorities at the local, state, federal, and Department of Defense (DoD) level to form a real time common picture, hence increasing the effectiveness, accuracy, and speed of the decision-making timeline. TCN integrates diverse capabilities into a system that allows the participating entities to speak and share information in a common language. All systems participating in NCR defense would share common track numbers, sensor updates, and intelligence information. This creates a fully integrated system that makes the Region's defense operate as a single identity. Furthermore, each level of command authority could share information in a peer-to-peer network using either automated machine-to-machine interfaces or an operator-in-the-loop structure. Information is shared in a "smart push" environment where individual users dictate the level of information they require in order to perform their specified mission(s). Once a response to an event is required, the data is developed and shared throughout the entire network, ensuring all participants have a common view of critical events.

NCR Scenario

Recent events in the nation's capital concerning both commercial and general aviation violations of restricted airspace have been greatly publicized around the world.

These capability gaps, either in sensor coverage or response time, have provided potential terrorists with valuable intelligence; they know what to expect from our air defense assets, understand system vulnerabilities, and noted tactics and response times. The DoD focuses its main defensive effort against air threats; the US Coast Guard focuses on maritime operations; and the police have focused on vehicle/tractor trailer movements. But nowhere do they combine this information to develop a complete picture of the entire Region. Each separate operation creates its own view based on the limited sensor inputs or information that has been developed within their system.

When the military controllers are directing fighter aircraft to intercept an inbound Target of Interest (TOI) neither the U.S. Coast Guard nor interagency departments such as the U.S. Customs or U.S. Secret Service are seeing the same picture of the ever-changing dynamic event. Additionally, there is no consolidated response or "plan of attack" to either try to neutralize the threat or respond if it is successful. Using a Mission-Centric Network (MCN) capability such as TCN, each node or agency could exchange data in real-time allowing first-responders to have greater situational awareness of critical events when they deploy to and approach the incident scene. Using TCN, the TOI that is detected and tracked by DoD is then relayed to all agencies on the network. This allows a coordinated response based on a high level of situational awareness by all first responders. Response time to threats is shortened and the opportunity of injuring non-participants is greatly reduced.

The Seven Cornerstones of Sensor Networking

For a network to meet each user's needs, it should conform to the seven cornerstones of sensor networking (as a minimum). These cornerstones are:

1. Network extensibility must be minimally impacted by the number of network participants.
2. Network participants must maintain physical and functional independence.
3. Each network must be responsive to diverse user needs.
4. Network data communication structure must seamlessly include all wireless data paths.
5. Multi-level data access must be supported.

6. Sensor elements must act in concert to meet user-specified objectives.
7. All element-specific processing must be performed at the originating elements and not at the recipients.

The TCN architecture allows for the extensibility of the network but does not eliminate a node's ability to perform its individual mission. This is achieved through what can be described as "smart push" arrangements. Each participant on the network defines its requirements for information and the level of fidelity required. This allows for several layers of users to operate on the same system without overloading each other or the network with extraneous information. User-defined independence ensures that a change to or the addition of any network element does not force a change to any other network element(s). As networks grow they include more elements and a greater diversity of element participants; this increases the pool of information available for making tactical level decisions. This can be compared to a telephone system, which is a simple model of an extensible and independent network [1]. Since the network is flexible, information can be shared as easily between command centers as well as directly to a single responder. Through a Personal Digital Assistant (PDA) or Pocket PC, the individual or first responder team can receive real-time updates or share information with their command center through a standard wireless network.

Communication flexibility permits users to interact on their traditional networks. In typical sensor networks, the need for high-bandwidth throughput dictates specific solutions. The TCN architecture can function in low-bandwidth environments; this provides the ability to function in a wide range of heterogeneous networks [2]. Participants with dedicated land lines are able to interact with wireless users who may be deploying inside the NCR. This allows users who have first-hand knowledge to notify the network of real-time events as they unfold and provide immediate feedback on developing situations. Since network communication is flexible, upcoming communication changes and upgrades can be planned, and the fidelity of information during the timeframe can be adjusted in an orderly fashion. TCN accommodates the differences in communications throughput in a seamless and fully interoperable manner; allowing users to use existing or select new communication devise(s) according to needs.

Multi-level access protects the source and fidelity of data so that providers can determine which end-users can obtain or will have "rights" to the data [2]. This is extremely important as we look at integrating law enforcement and intelligence agencies into the network. The levels of security and information release concerns have been addressed in the TCN architecture. TCN provides all coordinates in an absolute coordinate frame that does not identify the location or capabilities of the sensor source. This permits the inclusion of coalition elements, controlling access to their information without undermining legitimate user needs. Information can be provided to specific users without having it available to all users operating on the entire network. TCN provides for the heterogeneous interconnection of a variety of tactical, network-enabled applications. This is also important when combining law enforcement agency databases with the DoD databases. Due to federal law, much of the information maintained in U.S. Customs, Federal Bureau of Investigation (FBI) or other inter-agency databases can not be released to military personnel. TCN allows for the deletion of that data through permissions established by the data's provider to one participant while allowing another participant on the same network to receive the information.

To minimize bandwidth usage, redundant information should never be exchanged on the network. Exchanges must be made collaboratively and within the context of information provided by other contributing elements. TCN users cannot flood the network with information that does not enhance the current state of events.

The Tactical Component Network

TCN technology transparently integrates sensor and communications suites with distributed network applications. It is an enabler for time-critical, needs-driven applications where automated collaborative solutions are required from many users working with diverse sources of information [3]. The beauty of a TCN solution is that it accommodates legacy systems and facilitates an orderly migration to a well-defined component architecture that can be maintained and extended.

TCN has a local component, called the TCN Local Network that handles time-critical, peer-to-peer applications, and a wide-area capability called the TCN Global Network. The local TCN network provides the fabric for the network-centric grids; it

allows the individual peer networks used by fire, police, military, and medical response teams to interoperate in a given geographic area. Wide-area coordination can then be facilitated by a Hub-and-Spoke architecture tying local geographic networks into a global network; this capability is implemented by the TCN Global Network [3].

Local networks can be limited in range and by technology. The Hub-and-Spoke architecture provides a means by which local TCN networks can interact with each other and stored, value-added information. Through the use of a Hub, local entities are provided a global reach, participating in the fabric of the multi-tiered global information grid. The connection of Local TCN networks to the Hub is shown in Figure 1 [3].

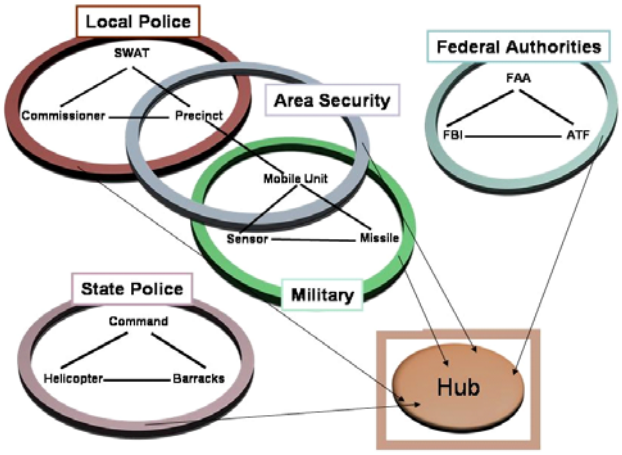

Figure 1 - Local and Global TCN

TCN provides an open-architecture approach to creating a network-enabled tactical environment, delivering information to users based on their needs for mission execution. It supplies data information knowledge to network consumers while minimizing the bandwidth requirements on landline and wireless communication links. To minimize both data distribution on the network, as well as the processing requirements of participating systems, the "needs" of an individual user drive data distribution bandwidth. Rather than distributing all data to all participants in the network, data users receive the amount and type of track data they request or types of data for which they register and are approved. Processing load is reduced because of fewer input interrupts. In a TCN-enabled architecture, each sensor and all communication devices act

in concert to create a collaborative picture of the environment. While used most often for creating a single integrated air picture, TCN can be applied to any discipline where the uncertainty of remotely sensed data can be characterized analytically [2]. Even though it was designed for military operations, it is easy adapted to the civilian arena, providing first responders with an avenue to share and collaborate their piece of the puzzle in an IDS without compromising their or the military's concern for the security of its data.

TCN Architecture Overview

TCN has, as its foundation, a collection of generic software applications including Data Conditioner, Current Observation Related Estimate (CORE) Synthesis, Extrapolated Fusion Algorithm Combined Track (XFACT), Multi Source Correlator Tracker (MSCT), Visualization (Tactical Display Framework [TDF]), and Messaging. A notional TCN structured is shown in Figure 2 [1,2].

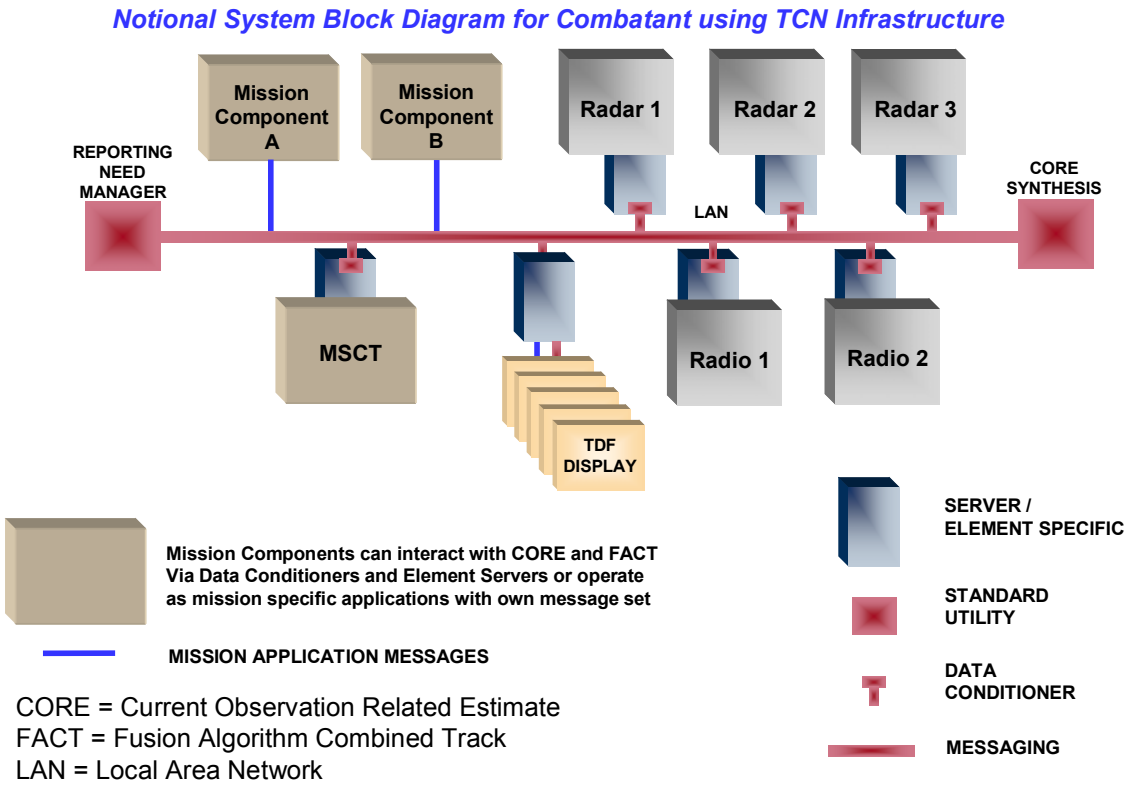

Figure 2 - TCN Segment

Within the TCN framework, the network processes are decomposed into common components. The components are designed so that data sources and consumers can be added without changing other components in the network. Standard utilities link the dissimilar data sources and consumers. As shown in the notional diagram (Figure 2), the data sources and consumers are linked to the network through components called servers. The servers are designed specifically for the network participant and will enable the participant to communicate using a common message language recognized by the network. A TCN-networked sensor exchanges information with the rest of the network through a component called a Sensor Server. The Sensor Server sends the data to a Sensor Data Conditioner (SDC) through an Application Program Interface (API) common to all participants in the network. The SDC accumulates and condenses the data into CORE. The SDC provides the data to the network based on the user-defined needs level of the track. CORE Synthesis then fuses the CORE with the appropriate network track and distributes a FACT to all users on the segment that have requested and have been approved for the specified track data. Data Conditioner and CORE Synthesis are standard network utilities common to all segments while the Sensor Server is a network component unique to the sensor. Components such as visualization (TDF), legacy system tracking, and correlation (MSCT), threat evaluators, or identification can be attached to a local segment or a TCN Global Network Hub to provide value-added services. This also allows legacy, non-TCN-equipped participants to interact with TCN participants and allows for a smooth transition during the TCN fielding process [2].

TCN architecture is an operational architecture that is being employed by the U.S. Navy and Air Force; it can be adapted to meet the challenging mission of defending our nation's capital and leaders.

Approach and End Result

Since TCN is based on users pulling data by describing their precise needs, hundreds or thousands of end-users can obtain the information required at the proper fidelity and in time to accomplish varied missions. The system is scalable and can be made affordable for a wide variety of applications because of the low-bandwidth requirements.

In this scheme, motorcades could have an air surveillance picture of their immediate airspace as well as roads depicting alternative routes. Nuclear power plants and other high-value assets could obtain surveillance data for their immediate area, and individual buildings could subscribe to receive sensor data in time to make a proactive response to a terrorist threat [4].

This can all be accomplished with a phone and a PDA or laptop computer and user-specified level of encryption. Figure 3 is a screen capture of the information that is available to a laptop computer user. The display available on a PDA is shown in Figure 4.

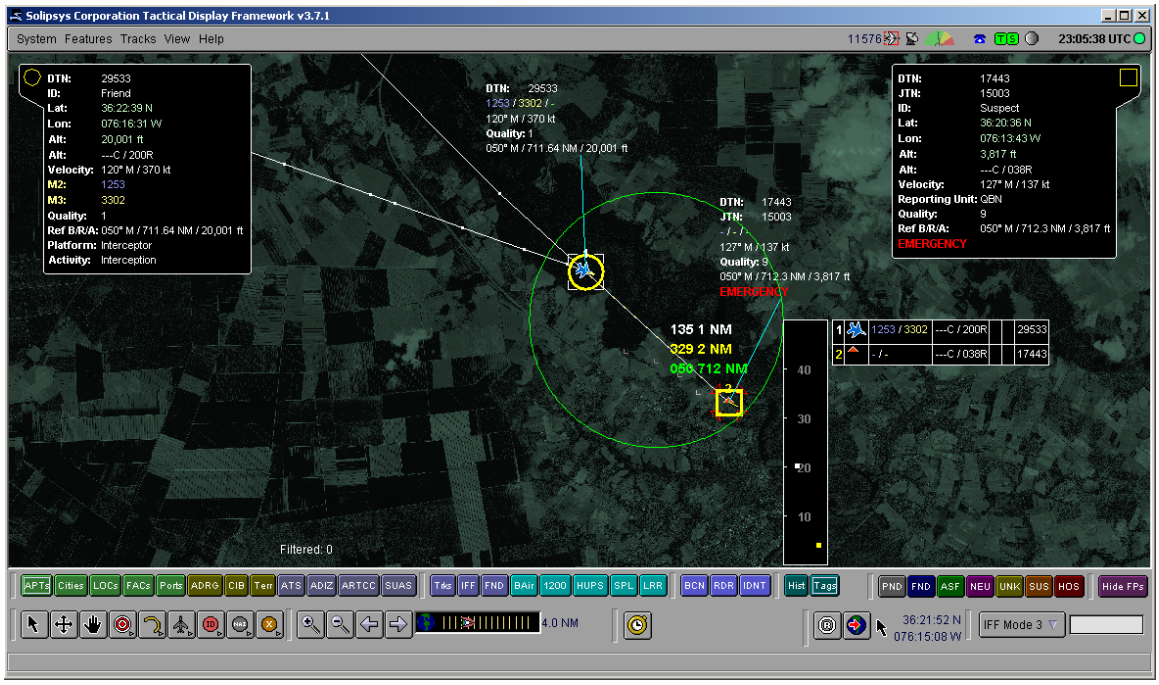

Figure 3 - TDF Laptop Screenshot for TCN

Figure 4 - TDF PDA Screenshot for TCN

Larger applications can be implemented in conjunction with sensors on individual platforms, large sensor suites used for Homeland defense, or in fixed or mobile applications. A new local or worldwide application can quickly be made operational via a TCN Local or Global Network, and all such instantiations can work together as required.

No longer will a problem seem intractable from the outset, because TCN applications are completely scalable [5]. The system can track and report on trucks, sea-going cargo containers, and ambulances as easily as it can track large quantities of airplanes. Instead of building a complete new system that might be cost prohibitive to perform these mission applications with TCN a user would only require a user terminal and communications interface to join the network and receive the information.

Current TCN-enabled applications

TCN is currently installed in several ships of the US Navy's 7th Fleet and also has been interfaced with E-2 and P-3 airborne surveillance assets. This architecture was also implemented for exercise Foal Eagle 2002 and Cobra Gold 2002. Figure 5 shows several levels of networks that performed successfully during exercise Cobra Gold 2002. Local Area Networks (LANs) connect TCN elements on a platform; wireless networks connect platforms within LOS of the radios; and a Wide Area Network (WAN) employing TCN

Global Network technology, uses the Iridium satellite constellation, can connect any platform, anywhere, anytime [2].

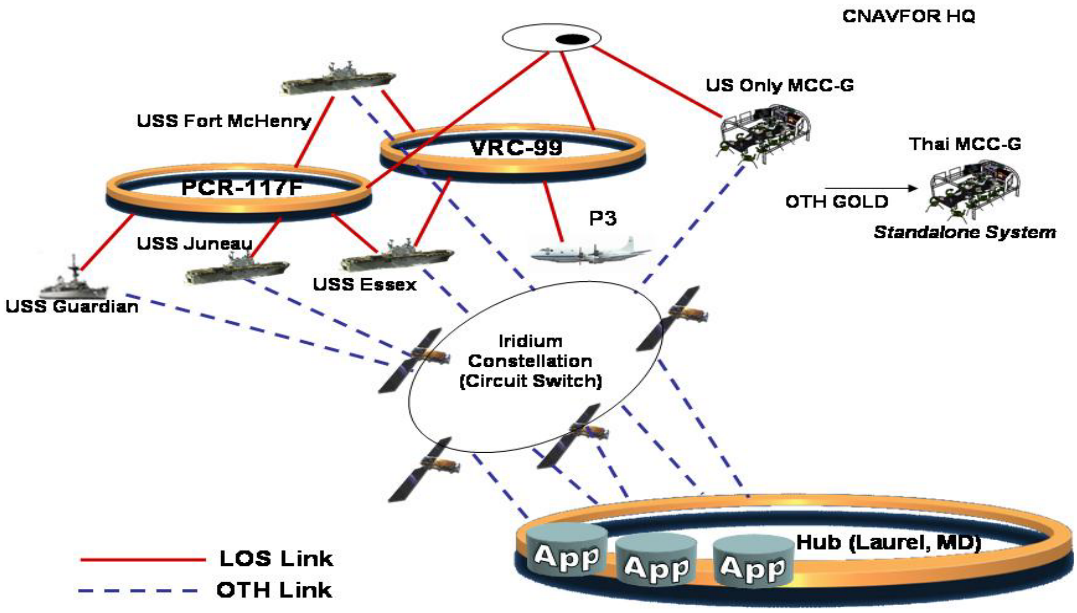

Figure 5 - Cobra Gold Configuration

This same basic architecture could be deployed in the NCR without modifications. Command centers could share information among different internal users using standard LAN connections. Local DoD players could share information across standard UHF radio waves through the TCN network or by Link-16 using TCN's MSCT gateway. Local police, firefighters, and other first responders could have the information distributed via wireless communications directly into a laptop or PDA in their patrol cars and command vehicles. During a time of crisis, when power for local cell phone towers and thus communications might be lost, users could still be a part of the network by using the Iridium satellite network, which would be unaffected by local power outages.

After the events of 9-11, North American Aerospace Defense Command (NORAD) selected two components of TCN (MSCT and TDF) to immediately eliminate its greatest shortfall in our nation's air defense by integrating the FAA CONUS internal radar into the NORAD air defense system. The NORAD Contingency Suite (NCS) was deployed to NORAD's three Sector Operations Control Centers (SOCC) and its Air

Operations Center (AOC). NCS is still operational today at all four locations [4]. Those two components have also been installed in the Joint Air Defense Operations Center (JADOC) at Boling AFB, which provides for the air defense of NCR. This system could easily be expanded to include more TCN functionality and would be an excellent foundation for incorporating local authorities in an NCR Integrated Air Defense System (IADS).

In January 2004, MSCT and TDF were deployed to the Baghdad International Airport to support the Control and Reporting Center (CRC) located in theater. US Central Command (CENTCOM) requested this capability to fuse the sensors deployed in theater and then feed that information into the CRC. This gave the CRC an enhanced air picture with greatly extended range within the theater. The MSCT and TDF were deployed in a mobile transient case configuration. Figure 6 shows the MSCT and TDF located in a tent in Baghdad, Iraq.

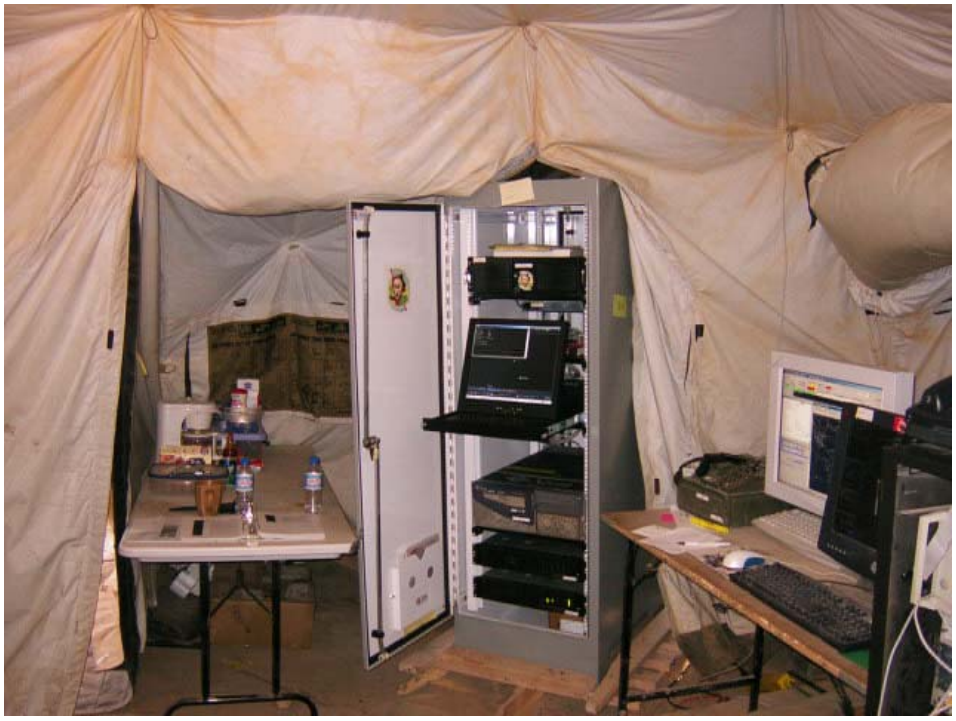

Figure 6 - MSCT and TDF Deployed in Iraq

Conclusions

Our nation's capital deserves the best integrated defense system in the world. TCN provides a simple, low-bandwidth architecture with the inherent flexibility required to develop an integrated defense network. TCN allows sensor systems and users to operate in a real-time data environment to deter terrorists from attacking our nation's capital. It also provides the capabilities necessary to respond to an attack by quickly expediting the direction and flow of defensive assets and resources to the point of attack.

The open architecture and plug-and-play components that comprise TCN are applicable across-the-board in Homeland Defense applications [3]. The ability to view and interact with a real-time air picture is critical to many terrorist threat scenarios; however, the integration of other databases and providers of vital information can quickly expand the utility of the system and the distribution of data, in near-real-time, to additional sites. Law enforcement and DoD can share information, within the limits of the law, in a netted environment. TCN is the "internet of tactical systems" with the specialized knowledge and flexibility to handle the types of situations in such an environment [5].

Future Work

All agencies with data pertaining to the NCR should be incorporated into a plug-and-play TCN architecture, operating in a manner similar to the way a Carrier Battle Group operates. The initial goals of the NCR should be to integrate military forces' sensors into a seamless C2 architecture using TCN. This should be followed by integration of the FAA, U.S. Coast Guard and U.S. Customs sensors into the network. Finally, first responder air and ground elements should be incorporated into the network. This would allow all interagency endeavors to support missions such as the protection of the President, special security events, and times of national crisis. The architecture remains the same as players and capabilities are added and subtracted based on mission execution needs.

References

[1] Solipsys Corporation, “TCN White Paper”, (12 December 2003)

[2] Mike Abrams, David Buscher, Paul Giaccio, and Bob MacKenzie, “Tactical Component Network (TCN) – An Enabling Network-Centric Technology for Homeland Defense”, Government Microcircuit Applications & Critical Technology Conference (GOMAC), April 2003, Tampa, FL.

[3] Margaret McMahon, and David Buscher, "A Hub-and-Spoke Architecture for Netcentric Operations (Urban Security)", Government Microcircuit Applications & Critical Technology Conference (GOMAC), April 2003, Tampa, FL, paper 09-04.

[4] Eric Conn, Steve Lee, Eric Firkin, and David Buscher, “NORAD Contingency Suite (NCS) – The Frontline in Homeland Air Surveillance and Defense”, Government Microcircuit Applications & Critical Technology Conference (GOMAC), April 2003, Tampa, FL.

[5] Solipsys Corporation, “Introduction to the Solipsys Tactical Component Network,” (15 March 2000)

Biographies

Eric C. Firkin is a former USAF Air Battle Manager with more than 24 years of experience in the Command and Control domain. He retired from the USAF in January 2003. During his career he served as a Commander, Director of Operations, and Mission Crew Commander in several units in the Ground Theater Air Control System (GTACS) which included deployments in South America, Southwest Asia and the Korean peninsula. Prior to his retirement he served as Chief, C2 Operations and Systems Branch, Air Force Command and Control, Intelligence, Surveillance, Reconnaissance Center (AFC2ISRC, Langley AFB, VA were he was responsible for the modernization and sustainment of the GTACS community. He currently serves as the Director, USAF Business Development for the Solipsys Corporation and is responsible for all USAF Programs for the company.

Margaret McMahon has more than 22 years in defense engineering and defense-related activities. Her experience in aircraft systems specification and testing gives her practical insight into the issues facing incorporation of technology in a military environment. She has extensive experience in the engineering and testing of the F/A-18, AV-8B, and A-10A aircraft. This experience is from both Government and contractor perspective and has yielded numerous scholarly publications. While at the Naval Air Warfare Center in China Lake, Dr. McMahon served as Advanced System Program Office Engineer, defining requirements for Special Programs using studies combining technology, tactics and fleet realities. Her advanced systems studies involved leveraging these studies to quantify the benefits of future systems. As an Assistant Professor at the US Naval

Academy her research in network security has specialized in authentication and ad hoc networking. She teaches basic and advanced network courses to future Naval Officers. Dr. McMahon's current research involves the implementation of network-centric technologies and includes consultation for Raytheon Solipsys in both Laurel, MD, and Kauai, HI. In this capacity, she is responsible for defining requirements for global Tactical Component Network (TCN) and has developed use cases to demonstrate how this architecture would support Ship-to-Objective-Maneuvering (STOM) tactics.