Systems Approach to the Army's Evolving Role in Support of Civil Authorities

John V. Farr, Eirik Hole, and John H. Gully
Professor and Lecturer, respectively, Department of Systems Engineering and Engineering Management, Stevens Institute of Technology, and Senior Vice President and General Manager of the Tactical Systems and Solutions Business Unit with Science Applications International Corporation

---

Abstract
The attacks on the World Trade Center and Hurricane Katrina have caused the total Army to reevaluate it responsibilities in support of homeland defense, homeland security, and defense support of civil authorities. Though the Department of Homeland Security has the lead in these mission areas, the U.S. Army plays a visible and key support role. The breakdowns that occurred in the past were the result of emergency responders and governments at all levels not understanding their dependencies and the essential functions that must be performed. In order for the Army to adopt tactics, techniques, and procedures and provide the necessary technical solutions, a systems approach must be taken to first define the role, missions, and responsibilities – from which training, personnel, and technical solutions can be developed. The results of a high level systems modeling effort will be presented to demonstrate the first step in a systems process of developing operational views derived from use case scenarios of an overall architecture.

Key Words: systems engineering, defense support to civil authorities, architecting

Introduction
The active, reserve, and national guard components of the Department of Defense (DoD) have a long and proud history of supporting non traditional operations. As shown in Exhibit 1, this can encompass a wide variety of missions. In the post aftermath of the World Trade Center and Hurricanes Katrina and Rita and the emergence of the Department of Homeland Security (DHS), the DoD role in and priority of supporting these types of operations is under scrutiny.

The primary mission of the DoD is to fight and win the nations wars. Given that the DoD, especially the Army, is engaged in a wide range of operations throughout the world, they do not have the resources to train and equip for these types of missions. As a result, the DoD was specifically criticized in a post Katrina assessment by the U.S. House of Representatives (2006) for:

• DoD/DHS coordination was not effective,
• Communications between DoD and DHS, and in particularly the Federal Emergency Management Agency (FEMA), during the immediate week after landfall reflect a lack of information sharing, near panic, and problems with process,
• DoD, FEMA, and the State of Louisiana had difficulty coordinating with each other, which slowed the response,
• National Guard and DoD response operations were comprehensive but perceived as slow,
• The DoD has not yet incorporated or implemented lessons learned from joint exercises in military assistance to civil authorities that would have allowed for a more effective response to Katrina, and
• The lack of integration of National Guard and active duty forces hampered the military response.

Despite these concerns, that bipartisan committee review of Hurricane Katrina, lauded the DoD for its efforts in the largest mobilization of military troops on U.S. soil since the Civil War.

Most of the issues raised in that report can be lumped under the broad Army term of command, control, communications, computers, and intelligence, surveillance, and reconnaissance (C4ISR).

The U.S. Army is currently undergoing a major transformation titled the Future Combat System (FCS) with these elements being the center of the transformation. The FCS is a $127B system of systems (one large system made up of 18 individual systems, the network, and most importantly, the Soldier) connected via an advanced network architecture that will enable joint connectivity, situational awareness and understanding, and synchronized operations (Program Manager, 2005). The FCS is being envisioned as a System of Systems (SoS) that will network existing systems, systems already under development, and systems to be developed

to meet the requirements of the Army's future. The FCS SoS are connected to the C4ISR network by a multilayered communications and computers network. From a doctrine, training, and equipment perspective the total Army (active, Guard, Reserves, and civilians) must ensure that current and future forces can respond to these critical non traditional missions and that all equipment is interoperable with first responders, DHS and other non DoD agencies.

The paper will present the methodology we used with emphasis on what are the requirements for the Army in the homeland security/homeland defense/defense support to civil authorities (HS/HD/DSCA) arenas. Secondly, given that we know that C4ISR is a major issue, how do we identify capabilities shortfall between SoS and the emerging HS/HD/DSCA mission – especially from an interoperability perspective.

Methodology

The first step in developing the requirements and subsequent architecture – from which shortfalls, interoperability, etc., are derived - was to adopt and follow a structured process. It became apparent early that the whole HD/HS/DSCA problem was an enterprise level problem with the Army being a stakeholder (see Exhibits 2 and 3). Given that the focus of this effort was on Army issues, we treated the problem as a SoS level effort and followed the approach shown in Exhibit 4.

As shown in Exhibit 3, the HS/HD/DSCA arena can best be described as Enterprise SoS because of the lack of central control, no clear or defined authority, and can be described as a complex adaptive system.

Interoperability is one of the biggest challenges for an Enterprise SoS because of time and geospatial alignment, publish and subscriber management, lack of omnipresent protocols, and passing and fusing of disparate information. Programs such of the FCS have standards and a common operating environment, though technically challenging, do not approach the magnitude of this problem.

There are numerous players, systems, domains, and enablers in a disaster relief effort. State and local agencies rely on commercial land-based mobile radio systems, and are increasingly depending on cell phones, internet, VCT, and web browsers. When a disaster strikes, certain critical infrastructure is lost. Hurricanes Katrina and Rita destroyed an unprecedented portion of the core communications infrastructure throughout the Gulf Coast region. The storm debilitated 911 emergency call centers and disrupted local emergency services. Accordingly, the communications challenges across the Gulf Coast region in Hurricane Katrina's wake were both a problem of basic *operability*, than one of equipment or system *interoperability*. DoD, because of its warfighting expertise, can establish stand-alone secure communications networks anywhere in the world, and is the most capable player in such a disaster to establish communications between all players.

Requirements

Early on we struggled with developing the requirements to develop a conceptual model of this system. We choose to conduct a quality function development (QFD) to help define the requirements. The process shown in Exhibit 4 was used to understand the requirements. As a first step we aggregated the 15 emergency support functions (ESF) used by the DHS (2004) in to 8 to make the QFD waterfall more manageable. This QFD exercise provided a structure means for developing high level requirements.

QFD Waterfall turns opinion into action. QFD is a consensus building tool that assures that details are not overlooked. By using the Army's three basic mission roles of HLD/HLS/DSCA and emphasizing the latter, a QFD systematic review addressed all the required ESF, as outlined by DHS. The waterfall provided the six-sigma methodology to not only determine but also prioritize the tasks that are needed to carry out the ESF. The results from this QFD process drove the requirements for the Army's role in support to civil authorities.

Use Case Scenarios

The DHS has defined 15 national planning scenarios. Use case scenarios are critical in determining the intended use of the architecture. Obviously, the amount of Army involvement can be a function of the many things to include how well the state is prepared, the magnitude of the event, etc. Priority in developing the scenarios should be placed upon those with the maximum loss in human life

Exhibit 1. Non traditional military missions supported by the Department of Defense.

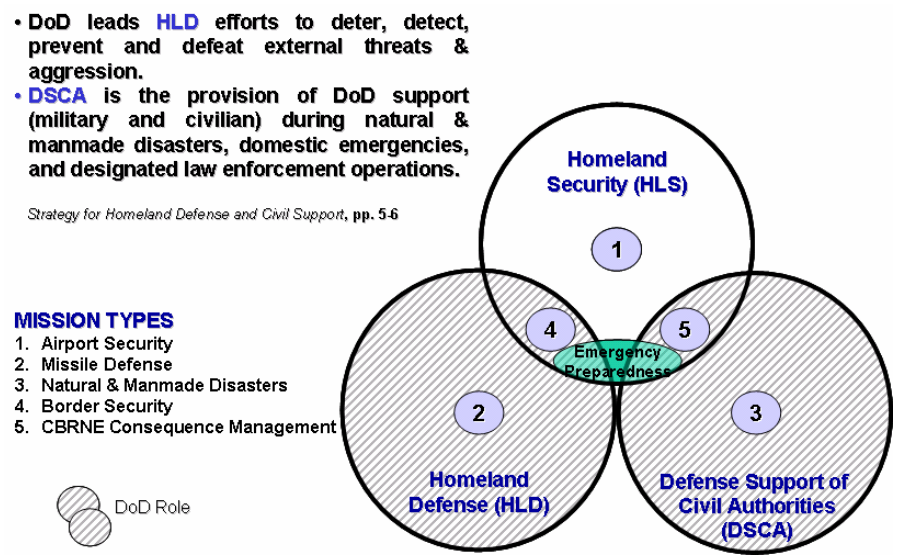


Exhibit 2. Systems methodology applied to enterprise level problems (from Checkland, 1999).

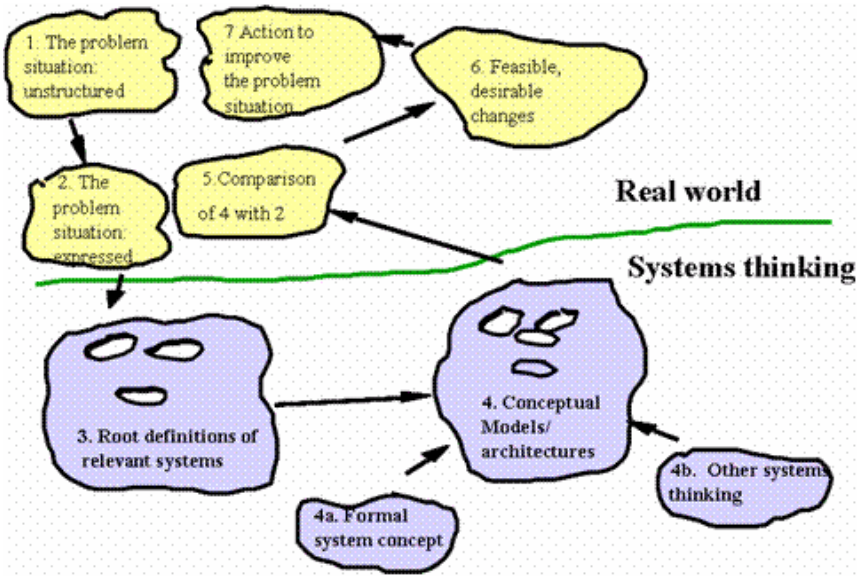


Exhibit 3. Enterprise SoS characteristics.

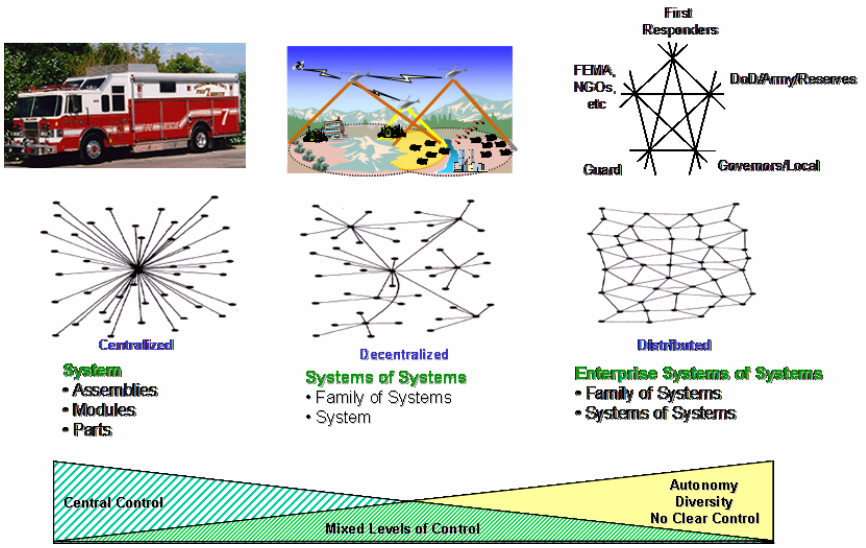


Exhibit 4. Systems process used in developing the architecture.

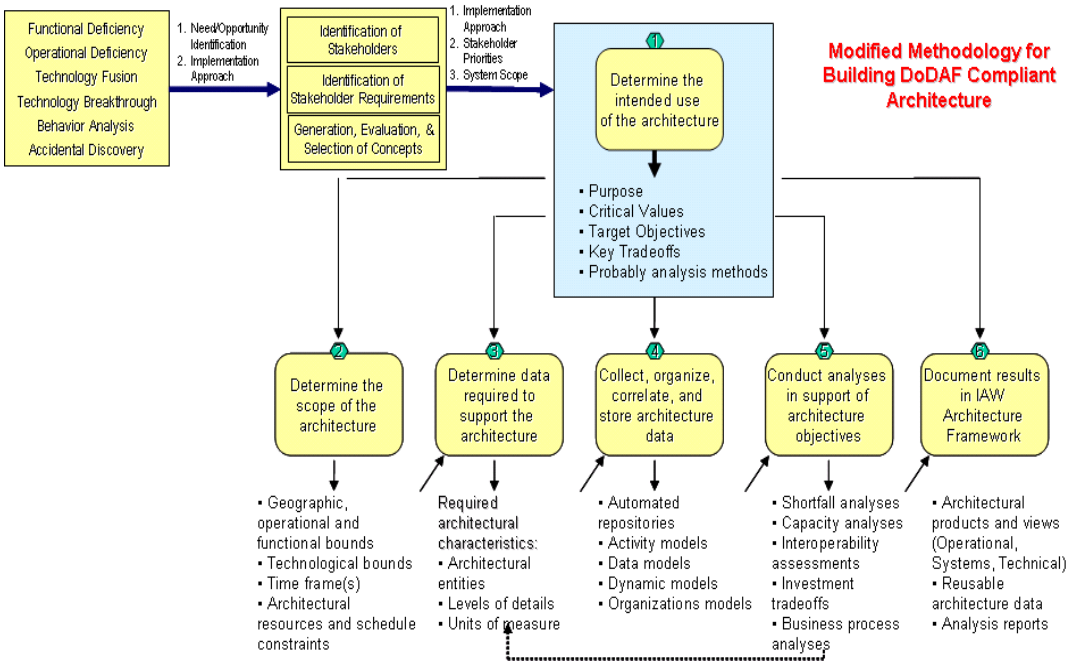
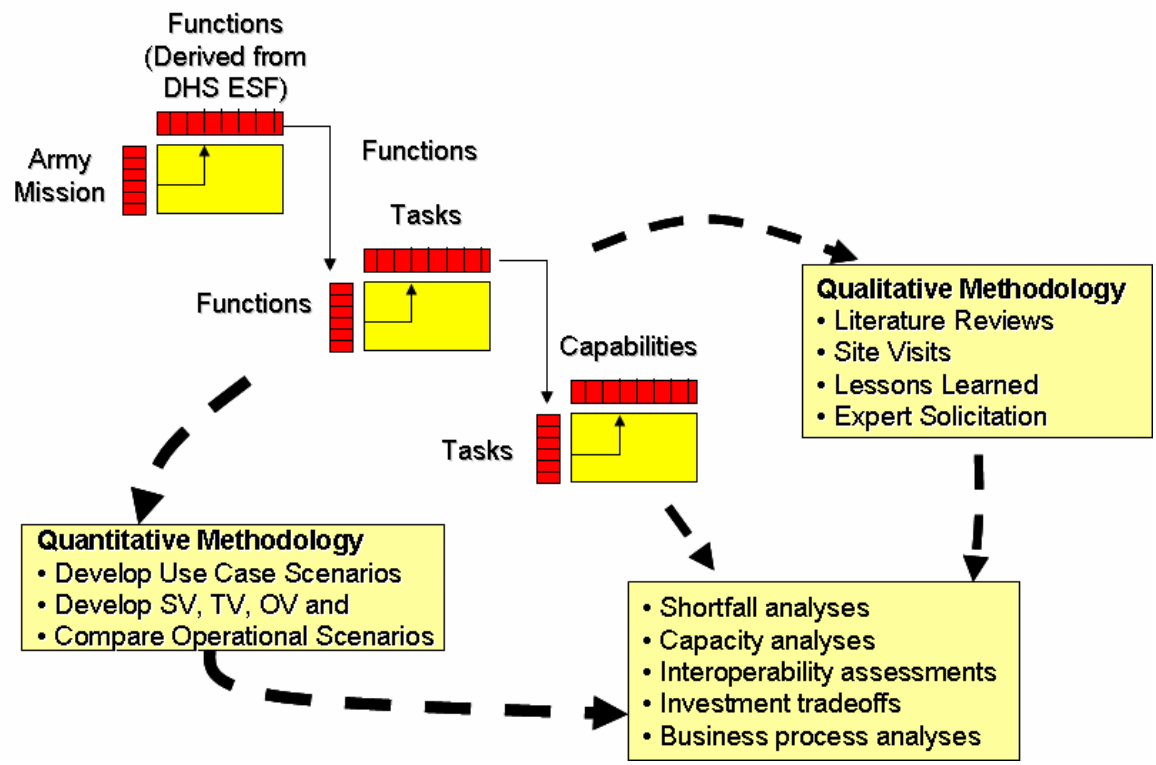


Exhibit 5. Process used in develop requirements.



Architecture

Most government agencies use some form of the DOD Architecture Framework (DODDAF, Department of Defense, 2003). The various elements of DODAF are shown in Exhibit 6. The DHS has proposed a draft standard title Public Safety Architecture Framework (PSAF, see DHS, 2005) which is very similar to DODAF. Exhibit 7 shows what an Operational View (OV) might contain. We are currently in the process of developing these views for scenarios that might require a major role and commitment of Army assets.

Summary

Authors often present papers in which they talk about following a "systems approach." The approach presented in this paper should be viewed as a textbook example of how to use systems engineering to architect a system of a very complicated system of systems. Follow on efforts will consist of developing detailed use case scenarios and build the systems models using the DODAF framework. From these "views" we hope to look at shortfall analysis, capacity issues such as communications spectrum, interoperability assessments, investment tradeoffs, communication processes, etc.

We believe that issues such as force design (for example the number of military decontamination units and equipment), capability needs (communications, cross training, force planning, etc.) and interoperability (the ability for first responders, the guard, regular Army, etc., to communicate under different levels of infrastructure damage), can only be addressed using an approach similar to the one outlined herein.

References

Checkland, Peter, "Systems Thinking, Systems Practice," John Wiley and Sons, 1999.

Department of Defense, "DoD Architecture Framework, Version 1.0, Deskbook," August 30, 2003.

Department of Homeland Security, "The National Response Plan," December 2004.

Department of Homeland Security, "The Public Safety Architecture Framework," The SAFECOM Program, February 10, 2005.

Program Manager, Unit of Action, "Future Combat System 18+1+1 Systems Overview," http://www.army.mil/fcs/whitepaper/FCS WhitePaper(v19_29Sep05).doc, dated September 29, 2005, accessed May 22, 2006.

U.S. House of Representatives, "A Failure of Initiative – Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina," February 15, 2006.

Exhibit 6. DODAF model building process.

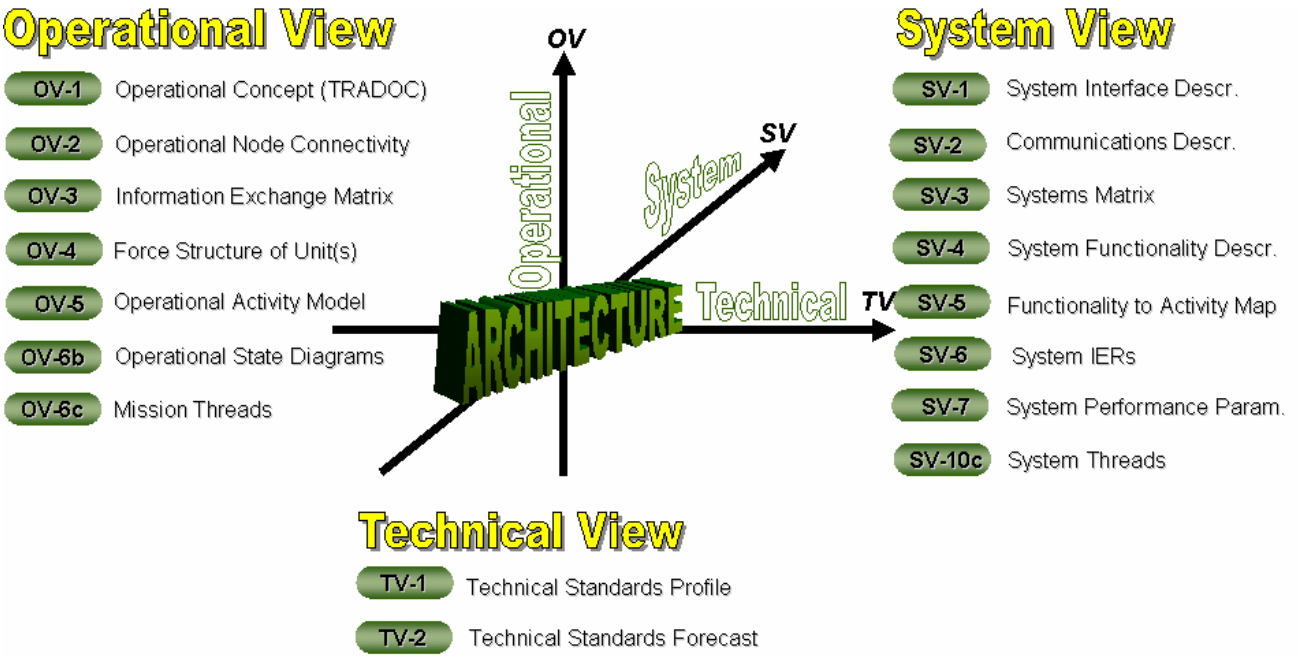
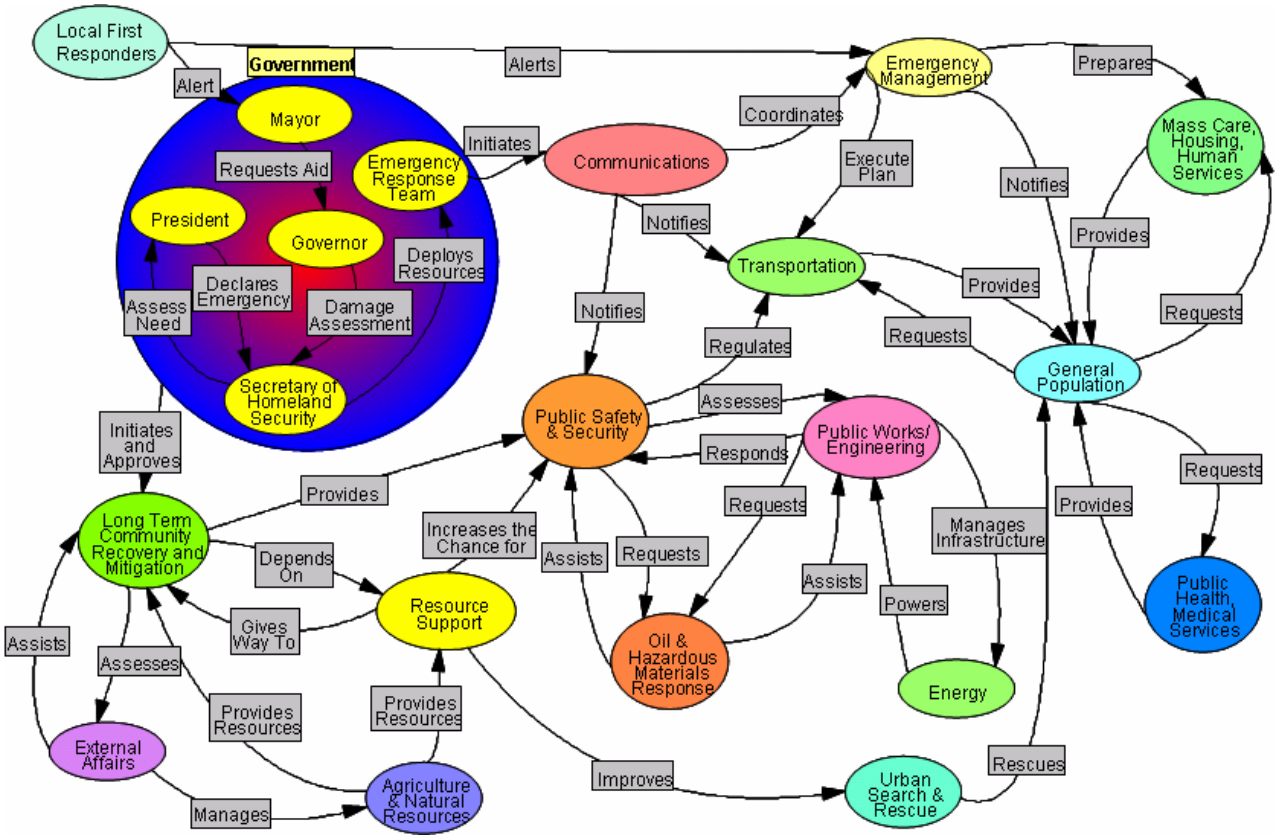


Exhibit 7. OV Level 1 architecture or high level operational concept.



About the Authors

John V. Farr is a Professor and Department Director, Department of Systems Engineering and Engineering Management, Stevens Institute of Technology. Before coming to Stevens in 2000, he was a Professor of Engineering Management (EM) at the United States Military Academy at West Point. He is a former past president and Fellow of ASEM and a member of the Army Science Board and Air Force Studies Board. He can be contacted at jfarr@stevens.edu, phone: (201) 216-8103, or fax: (201) 216-5541.

Eirik Hole is a Lecturer and Director of the Systems and Enterprise Architecting Laboratory at Stevens Institute of Technology. He received his MSc from the University of Stuttgart, Germany. Before coming to Stevens he worked for HOOD Consulting in Munich, Germany where he was implementing Systems Engineering and Requirement Management methodology and tools, mainly in the automotive industry. Before that he was a Systems Engineer in the aerospace and defense industry. He can be contacted at ehole@stevens.edu.

John H. Gully is Senior Vice President and General Manager of the Tactical Systems and Solutions Business Unit with Science Applications International Corporation (SAIC). Having joined the company in 1998, John develops and manages programs in SAIC's Training, Testing, Transformation and Logistics Group. The key focus of these programs include Future Combat Systems, hybrid electric powered combat vehicles, gun launched precision munitions, and tactical C4ISR. Prior to joining SAIC, John was Deputy Director, Tactical Technology Office (TTO), at Defense Advanced Research Projects Agency (DARPA) from 1994 – 1998. John also served as the Director, Center of Electromechanics, at the University of Texas where he directed advanced research for high power electrical systems, composite materials, mobility systems, and industrial process projects for military and commercial applications.