Proposing a C4ISR Architecture Methodology for Homeland Security

Monica F. Farah-Stapleton,
U.S. Army CERDEC
Fort Monmouth, NJ
Email:
Monica.FarahStapleton@us.army.mil

Dr. James Dimarogonas,
12 Christopher Way,
The MITRE Corporation
Eatontown, NJ
Email: jad@mitre.org

Dr. Paul J. Deason,
TRADOC Analysis Center,
White Sands Missile Range, NM
paul.deason@us.army.mil

Rodney Eaton
TRADOC Analysis Center,
White Sands Missile Range, NM
rodney.d.eaton@us.army.mil

Abstract

This presentation presents how a network architecture methodology developed for the Army's Future Force could be applied to the requirements of Civil Support, Homeland Security/Homeland Defense (CS HLS/HLD). This architecture application design will demonstrate how to link the sensors, command and control, and communications systems of local, state, regional, national and DoD elements. The architecture definitions and specifications of the inter- and intra-agency links would be usable in real-world operations as well as enabling the representation of CS HLS/HLD scenarios within large-scale stochastic simulations (e.g., the Combined Arms and Support Task Force Evaluation Model (CASTFOREM)). Representation in detailed stochastic simulation allows the evaluation of the impact of proposed hardware or software before acquisition or fielding. This methodology can also be used to develop operational and contingency plans by evaluating different options for possible real world events.

1.0 Introduction

The *DoD Architecture Framework Version 1.0, Final Draft* [1] and its preceding work: *Command, Control, Communications, Intelligence, Surveillance, and Reconnaissance (C4ISR) Architecture Framework, Version 2.0*[2] developed by the Department of Defense (DoD) C4ISR Working Group provided the guidance for the establishment of the C4ISR systems engineering methodology developed for the Army's Future Force, including the Army Future Combat System (FCS). This paper describes the components of that methodology, i.e. Architectural Tenets, utilization of synergized Architecture Views, their representation in communications networking modeling and simulation for system of systems analysis, and applicability of this approach to elements of the Homeland Security Presidential Directive – 5 (HSPD-5) and the U.S. Department of Homeland Security's National Response Plan. Once the Framework has been developed to address the communications linkages supporting the responsible and responding elements in the area of Homeland Defense, this methodology and subsequent representations may be useful to first responders for planning purposes and for operational execution. For the purposes of this paper, the following definitions for Civil Support, Homeland Security/Homeland Defense (CS HLS/HLD) apply:

Homeland Security (HLS) *~ A concerted national effort to prevent terrorist attacks within the U.S., to reduce vulnerability to terrorism, and to minimize the damage and recover from attacks that do occur.*[3]

Homeland Defense (HLD) *~ The protection of U.S. territory, sovereignty, domestic population, and critical infrastructure against external threats and aggression.*[4]

Civil Support (CS) *~ DOD support to U.S. civil authorities for domestic emergencies and for designated law enforcement and other activities.*[5]

2.0 The Threats

The threats to modern societies including the United States Homeland—particularly to cities within —have changed in character and intensity. A dozen years ago the major global threat was large-scale military forces participating in protracted land battles, supported by sea and air power—or from nuclear holocaust, if mutually assured destruction (MAD) strategies failed. With the friction of the Cold War diminished, the major threat appears to be from other sources: lesser nation states, paramilitaries,

[1] *DoD Architecture Framework Version 1.0, Final Draft* January 2003.

[2] *C4ISR Architecture Framework Version 2.0* Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence, Washington, D.C., November 1997.

[3] National Strategy for Homeland Security

[4] Defense Planning Guidance FY 2004-2009

[5] Defense Planning Guidance FY 2004-2009

guerrilla groups, terrorist cells and techno-bandits. In addition to operational focus continuing overseas, we are also focusing within our shores to prevent foreign adversarial attacks on the homeland which may include (a) disruption or damage to the economy, (b) undermining the political will, (c) inflicting massive casualties or disrupting vital government and economic services, (d) disruption of power projection and denying access, thereby restricting the distribution of forces to foreign battlefields.

Threat targeting policy includes, and may in fact concentrate on, densely populated urban areas, whose victims will include civilians who are not familiar with the dangers recognized by members of a nation's armed forces. As early as 1975, Burton[6] (lecturer at Oxford and the British Staff College) pointed out that innocent bystanders were increasingly becoming the targets of revolutionaries and separatists, and offered a troubling report on the limited responses available to governments to deal with this "ugly, contemporary phenomenon." He stated "The problem is at root, one of intelligence…" Burton's concerns then were focused on less prepared terrorists than the ones we now face.

Given that modern crimes against peace or humanity may be the result of a dangerous subset of modern terrorists who are not deterred by death sentences, how does a democratic government protect its citizens, infrastructure, and economy? Needed to countermand these threats is a minimally intrusive means of monitoring change in large metropolitan areas—technology that provides warning and legal evidence of criminal or military activity that may threaten our national interests. While the debate continues regarding the circumstances under which the monitoring of the "health" of a region should be permitted, the technology exists to do so.

3.0 Concept

The purpose behind the development of the C4ISR Framework came from the Defense Science Board in the early-1990s. In order to develop an interoperable, economical, and comprehensive military system for use by multiple Services, a comprehensive C4ISR architectural guide had to be developed and universally applied throughout DoD[7]. The Framework would enable the Operational, Systems, and Technical architecture views developed by the Services, Warfighting Commands, and Defense agencies to be inter-relatable. The requirements imposed on the DoD by HSPD-5 and the National Response Plan highlighted the need to facilitate interoperability between DoD and agencies of the Department of Homeland Security, and by extension the Federal agencies tasked with the effort. Utilization of the DoD Architecture Framework enables extension of the DoD C4ISR architectures to the elements at the

[6] Burton, Anthony *Urban Terrorism: Theory, Practice and Response*. New York: Free Press, 1975.

[7] Architecture is defined as the structure of components, their interrelationships, and the principles and guidelines governing their design and evolution over time. This architecture would be similar to the command, control communication, computer, information, sensor, and reconnaissance (C4ISR) architecture being designed for the Army's Future Force (formerly referred to as the Army Transformation), to include the Future Combat System (FCS).

regional, state and local levels tasked with responding to disasters, whether natural or man-made.

This C4ISR architecture design would provide a framework to enable the linking of traditional DoD sensors, command and control mechanisms, and communications assets with the systems of local, state, regional, and national elements. The techniques adapted from the military studies would be used to identify the core interoperability elements necessary for standardizing the collection, management, storage, and retrieval of sensor data and information; and disseminating data and information in a timely, efficient manner in times of emergency and national crisis. A System of Systems (SoS) approach would be employed to tailor the response means and methods, as circumstances warrant and facilitate the use of a mix of current, off-the-shelf,, and future systems. As ISR, C2 and communications interdependency requirements for the CS HLS/HLD evolve, understanding the potential impacts to the wide variety of existing systems throughout the nation is crucial to successful C4ISR interoperability. The SoS architectures developed for the military would provide a baseline context and framework for sensor interoperability and extensibility to other sensors, systems, or circumstances in terms of a 'big picture' for the local, state, regional, national and DoD elements. Utilization of the data captured in C4ISR architecture framework products would enable the representation of CS HLS/HLD scenarios within large-scaled highly detailed military stochastic simulations. This representation in simulation would facilitate the development of concepts and policy, operational and contingency plans as well as allows the use of simulation tools in emergency situations to evaluate changes. Simulation would also allow the evaluation of the impacts of improvements and changes proposed to the HLS/HLD through the addition of new concepts, hardware and software before purchase or implementation.

4.0 Approach

The approach starts with defining a set of architecture tenets, i.e. guiding design principles, for the HLS architecture in question. This is based upon a careful examination of the specific HLS environment, interviews with subject matter experts from within the associated HLS agencies to provide an understanding of the environment in question. This exercise should also include experts from the Army transformation community who can provide the lessons learned from the various DoD initiatives that are relevant to the problem space. Once defined, this set of tenets will represent a candidate set of issues that would need to be resolved by the architecture, and will guide the rest of the architectural development. For C4ISR they have been separated into four broad categories: Overarching Tenets that span dependencies across the C4ISR problem space, C2 Tenets, Sensors Tenets, and Communications Tenets. These in general identify risk areas which must be addressed if the C4ISR architecture is to be successfully employed within the HLS operational environment. The following are examples of some tenets that have been identified from ongoing HLS related work:

- Overarching Tenets
  - Encryption
  - Intrusion Detection
  - C4ISR System Security
  - Priority Management
  - Interoperability

- Command and Control (C2)
  - Situational Awareness
  - Situational Understanding
  - C2 Messaging
  - Distributed Databases

- Sensors
  - Infrastructure Protection
  - Access Control
  - Easily Deployable Sensors
  - Sensor Management and Fusion

- Communications (Comm)
  - Urban Comms
  - Mobile Communications
  - Comm Relays
  - Adaptive QoS

4.1 Tenet Description Examples

The following are examples of architectural tenets for C2, Sensors, and Communications domains, as well as overarching tenets applicable to all three. It should be noted that there are several issues that apply to most HLS environments- security being one of the main concerns. As C4ISR evolves into a more visible role, it will also become a more attractive target for anyone intent on disabling HLS detection or response capabilities. Security is implicitly and explicitly included in the description of each HLS C4ISR architectural tenet, as illustrated in the examples below.

4.1.1 Overarching Tenet: Encryption

To avoid attempts at monitoring HLS activities, response metrics, capabilities, monitoring and detection techniques, voice and data encryption are critical at maintaining confidentiality of the operational information. Traditionally, this would be limited to the main communications channels, but in a C4ISR context these concerns should also address sensor data sources such as cameras, and biochemical detection devices.

4.1.2 Overarching Tenet: Intrusion Detection

Given a sound encryption strategy, mechanisms to enable C4ISR intrusion detection become imperative. More than the traditional monitoring system, intrusion detection must be an integrated command and control system which ties into the C4ISR infrastructure seamlessly to provide alerts when a system is being compromised or when it has already been compromised, block out the compromised system without alerting the intruder, and assist in coordinating the response to identify and apprehend the intruder .

4.1.3 Overarching Tenet: Interoperability

The HLS environment is traditionally a collection of multiple incompatible systems and components, developed by different agencies, with narrow mission focus, stove piped and non interoperable between agencies, or in many cases within agencies themselves. Interoperability of the C4ISR systems and components is absolutely essential to be able to exchange information across agencies, coordinate responses, and provide redundancy that can be leveraged across agencies when and where it is needed. Design with the larger picture in mind, use of open systems and standards, interface control agreements, etc, will be a critical part of any kind of HLS C4ISR system development

4.1.4 C2 Tenet: Situational Awareness

As attacks will become more and more sophisticated in the future, response capabilities must evolve as well. Good Situational Awareness (SA) is at the heart of any successfully deployed C2 system. SA includes both position and status of friendly elements, as well as threat elements. Information about civilians, infrastructure, traffic, emergency areas etc. must also be included, and displayed at the appropriate level of detail and fidelity based on a recipients' role, training, requirements etc.

4.1.5 Sensors Tenet: Infrastructure Protection

When access to the system is not possible, disruption or destruction of key parts of the C4ISR system may be attempted. The infrastructure must be comprehensively designed as part of the C4ISR system, to ensure that each subsystem is robust, tamper proof, and protected either by physical security or remote monitoring via sensor assets, such as cameras and biochemical detectors which are seamlessly integrated into the C4ISR system of systems.

4.1.6 Communications Tenet: Comm Relays

The traditional terrestrial communication network often needs to be augmented with terrestrial and airborne communications relays to provide connectivity throughout the required area of coverage. This is especially critical in the event that an attack has disrupted parts of the normal communications infrastructure, as was seen in the case of the world trade center attacks. Relays with multiple comm packages on platforms at multiple altitudes, highly reliable links to unmanned robotic systems, as well as systems that relay communications in subterranean environments would need to be employed.

4.2. Architecture Development Methodology: The Execution Matrix

Once the basic tenets have been established they will be used to guide us in including the appropriate stressing environments, missions and tasks to ensure that we can understand the requirements associated with these areas. Therefore we need to identify a scenario that will emulate a real life use of the system, while stressing the risk areas we identified in the tenets. Once a scenario is built or chosen, the constraints of the scenario need to be set. These include environmental conditions, time of day, weather, etc. which are used to set the stage for playing out the scenario. Reasonably stressing conditions are desirable, without trying to identify the absolutely worst situation conditions that would cause us to overdesign the system. We choose a set of conditions that would stress our system and assist the attacker as if the attacker would have reasonably chosen them . Once the scenario and conditions are chosen, then we decompose the scenario into vignettes. These are specific mission tasks that involve a number of elements in typical normal operations or response patterns. Pursuit of a terrorist is one example. At the same time another vignette could be a normal patrolling operation that is occurring and that now needs to interact with the pursuit. The vignette decomposition is designed to capture as many of the different elements that need to interact within the scenario and ensure that we stress as many of our systems as possible.

The first set of information we must develop/integrate is a force structure, which is captured in the framework in Operational View 4 (OV-4). This is simply the layout of entities contained in our HLS environment ranging from local police to city and state authorities, represented in a hierarchical diagram denoting the reporting relationships between the entities, as well as among the organizations. In the simplest case it is just a diagram of who is subordinate to whom. But in the case of the HLS environment, some agencies have much more complex relationships, and in general do not belong to the same reporting chain. In this case, we need to capture roles and responsibilities, and any established interfaces and collaboration agreements between the agencies to build a comprehensive equivalent of a military force structure. This will help us play out the scenario realistically and assign tasks to the appropriate entities, as it would occur in a real life situation.

We now have an understanding of the entities and their roles and interrelationships. In order to play out a scenario, we also need to have a zero order understanding of the capabilities each entity possesses. This includes vehicles, communications, sensors, command and control, weapons etc. So we need to take the list of entities captured in the OV-4 and associate a rough estimate of what systems each entity will have available. This is usually referred to as a systems book, which goes through each type of entity, or by platform, and identifies all the projected system capabilities associated with the said entity or platform.

Next is the creation of an execution matrix, which is comprised of rows containing a single friendly entity or platform. It's information can be captured in the framework as an Operational View 6c (OV-6c). The columns are defined as phases of the scenario, which roughly correspond to a time sequence of events that the scenario follows in its natural progression. For example the phases could include detect suspect, identify suspect, pursuit suspect, apprehend suspect. For each of the vignettes we start filling in the matrix with the actions that need to be performed by each entity within the context of the scenario, for each phase of the scenario. In addition to the tasks, we identify what information needs to be received or sent in order for the tasks to be executed successfully. Thus we build a matrix of all the actions and information flows that need to take place throughout the scenario. To successfully build the execution matrix, Subject Matter Experts (SMEs) that sufficiently span the scenario space must be utilized. Each of them must contribute their knowledge of: (1) How operations occur today and (2) Extrapolate as to how they could occur if the technologies identified in the tenets and in the systems book were available to the users.

The execution matrix now becomes the basis of the architecture development. We have identified the information flows, which we can then use to create the connectivity diagrams (Operational View 2) that identify the entities that need to communicate (and therefore have communication paths). By looking at the tasks, we can estimate what C2 and Sensor functionality must be present so that the tasks can be performed successfully. Now that we know the system functionality at the nodes, we can identify additional information about the information flows, based on the system capabilities at the node (e.g. a sensor would have specific characteristics for the data it sends back). By adding more details to the information flows, e.g. estimated message size, priority, etc we can extract the Information Exchange Requirements which are captured in the framework in the Operational View 3 (OV-3) between a producer-consumer pair. Once we have the OV-3, we can now start working towards a communications network design. Figure 1 illustrates the Architecture Development Methodology.

Note that the procedure for creating the execution matrix is the most critical one in the process, and requires the use of SMEs, to provide input in a well coordinated manner. The rest of the development depends on this step being executed as successfully and accurately as possible. Application of the right resources to ensure that as much operational information as possible is captured, cannot be over emphasized. Many times this important step is overlooked, and the result is usually a failure to capture the user requirements that would ensure a system design that meets their needs, and that can be successfully employed to complete the mission.

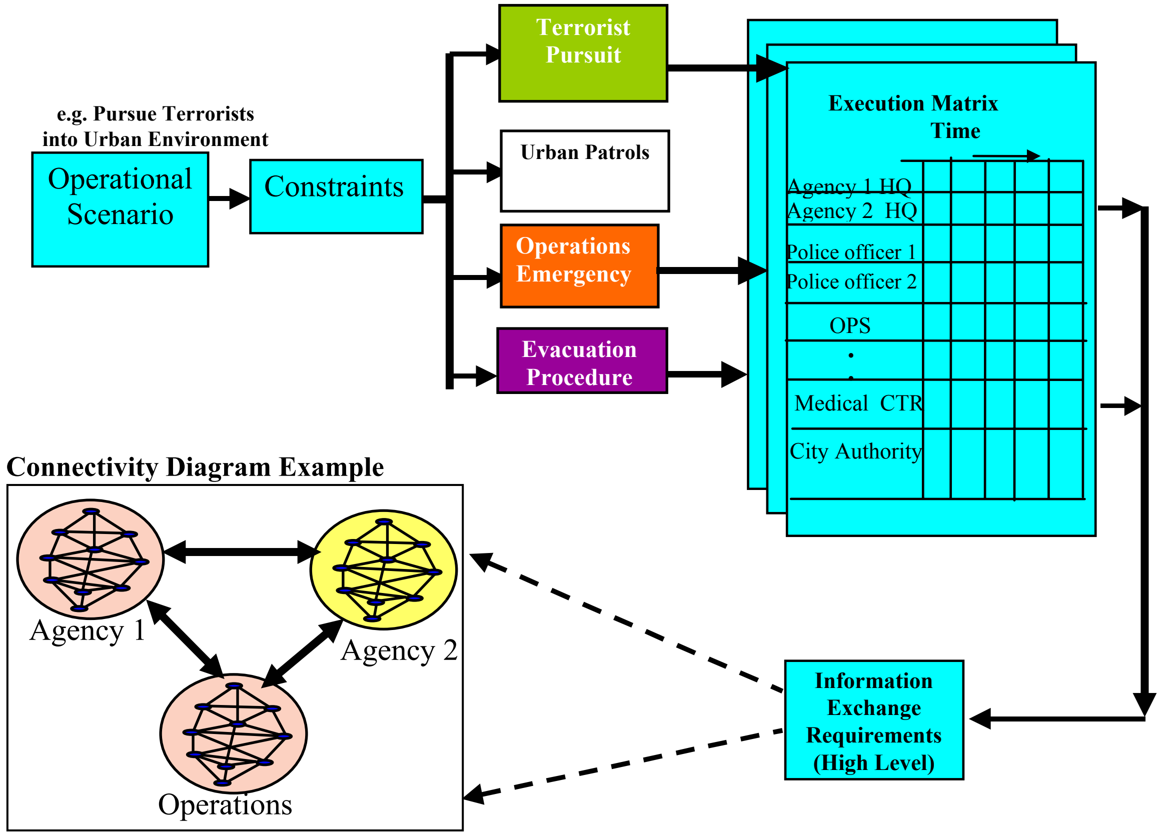

Figure 1. Architecture Development Methodology.

4.3 Developing System Level IERs

To identify a communications network design we need to know the following:

- How much information needs to be disseminated (e.g. how many messages, message size, etc.)

- Who sends it and who needs to receive it (producer-consumer pair)

- Where is the sender and receiver and how are they moving (mobility profiles)

- What are the requirements that need to be met by the information exchange (e.g. speed of service)

By “playing out” the scenario with its associated vignettes in the execution matrix we have identified the crucial elements of information that need to be exchanged. For each of those exchanges we have estimated metrics such as message size, priority etc, having established the OV-3 view of the operational requirements. But we know that these will not be the only traffic on the network. Other background traffic will be present, such as network routing, database replication, server traffic etc. Therefore another procedure is needed to estimate the actual “system” level traffic. Two approaches have been used in previous developments:

1. Use the operational traffic in the OV-3 and for each IER identify what the system overhead traffic would based on our knowledge of the protocols used. Code that information within an automated tool that now scans the IER database for certain characteristics within each IER, and attaches the overhead traffic for each one, based on a set of protocol rules.

2. In cases that protocols are not fully known yet, or to account for additional traffic we know has not been captured, we use SMEs to provide broad estimates of any additional overhead traffic. Their estimates can be based on field measurements, or experience from previous developments, or experience with use of the systems involved.

By combining the overhead traffic with the operational traffic, we generate System Level IERs, which are captured within the framework in Systems View 6 (SV-6). We now have the basis for sizing our communications network.

4.4 Communications Network Architecture Methodology

The IERs in and of themselves lack context. They simply represent the information produced by a certain entity, and the need for that information to be consumed by another entity. We need a method to layout in general terms the different networks and subnetworks which must be designed into the larger system of systems. This is achieved by taking the IERs, and based on a set of commonality criteria creating bins by which the IERs will be classified. As an example one bin could include IERs for which the sender and receiver are geographically co-located. Within that bin we could separate out which ones are mobile, and which are stationary. So now we have identified two possible subnets: One wireless subnet for the mobile geographically co-located nodes, and a LAN like subnet for the stationary co-located nodes. The commonality criteria usually include range, mobility, data rate, data service type, or any specialized requirements associated with the IER. All the IERs are ultimately grouped into these bins, and a high level picture of the network requirements starts to emerge. The result is the ability to lay out a notional decomposition of the network, which will help in conducting the detailed analysis necessary for creating a detailed design.

Once we understand in broad terms what the network will be, we can start performing analysis to determine the required characteristics of each part of the network. For example, for a possible wireless subnet, we would perform a propagation analysis, to identify ranges, relay positions, and achievable data rates. For fixed infrastructure we can perform simple analysis of the IERs to identify bandwidth requirements, or use tools such as OPNET or QUALNET to conduct a high fidelity simulation of the network and collect metrics to optimize the network design. The analysis will yield a more detailed network design, with specific parameters and metrics identified and calculated. All the information can now be captured in the Communications Architecture Description, which is mapped to the System View 2 (SV-2) framework product. This view contains the layout of the network as sets of diagrams of network equipment interconnections, but for these studies also contain all the analysis, the parameters settings, the estimates of the associated metrics, etc. Figure 2 illustrates the Communications Network Architecture Methodology.

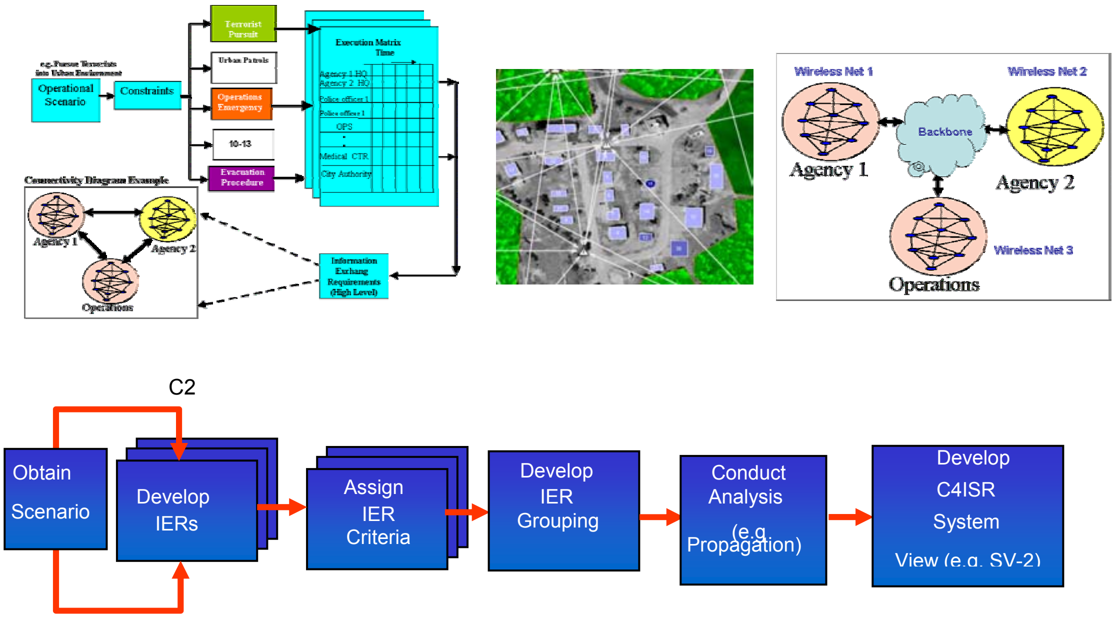

Figure 2. Communications Network Architecture Methodology.

4.5 C2 and Sensor Architecture Development Methodology

As mentioned previously, the execution matrix helps identify the necessary C2 and sensor capabilities. To arrive at the final C2 functionality description, other inputs must be included. Figure 3 illustrates the process to develop the C2 and Sensor functionality profiles.

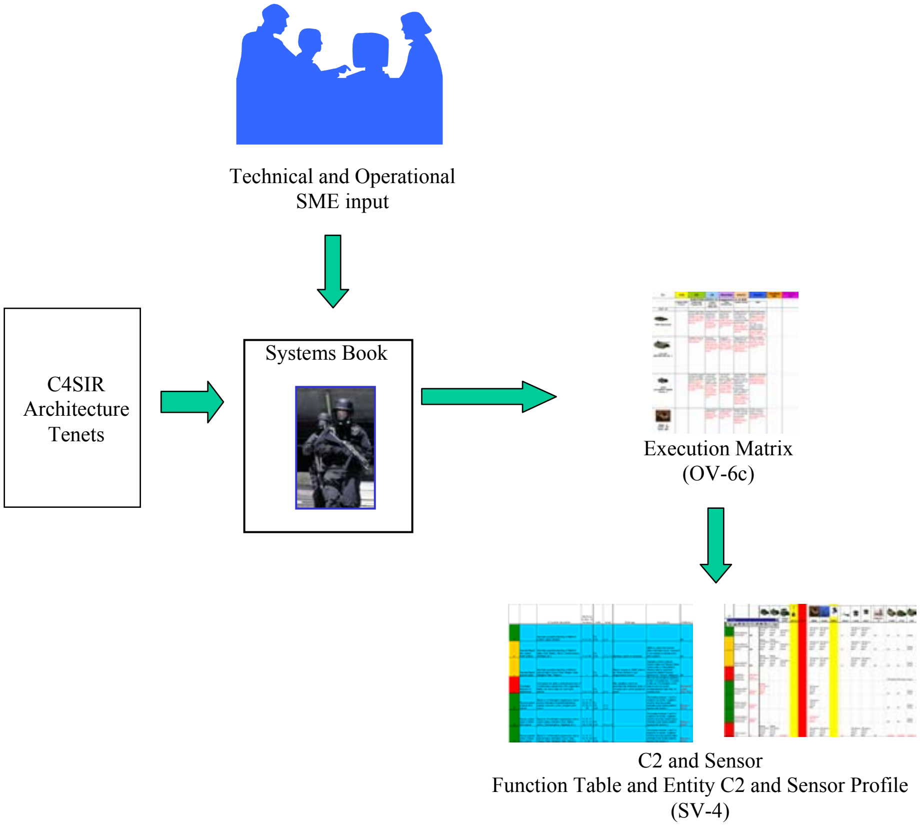

Figure 3. C2 and Sensor Architecture Development Methodology

As mentioned earlier, the foundation of our methodologies is the C4ISR architecture tenets. These are the guiding design principles leading to the identification of the minimum set of technologies which must be included, and some initial conditions/rules for their employment. From the tenets, and with the help of input from subject matter experts, and we create the systems book. The SMEs need to span both the technical and the operational spectrum in order to understand the functionality of the systems. The result is the preliminary C2 and sensor architecture. We then use this information to contribute to the development of the execution matrix as described earlier. For each step of the scenario, we identify if the capabilities each entity possesses are adequate, identify how each entity is employed, and what additional capabilities would be required to successfully complete the mission. These are included in the comments in the cells of the execution matrix. From this information, we are able to decompose each capability into its basic C2 and sensor functions. For example we will identify that certain types of sensing functionality is needed by certain entities of the force structure; that C2 functionality such as situational awareness is necessary everywhere, but mission planning tools are only required for certain entities; or that functionality for controlling unattended systems such as remote sensors are needed by certain entities in the scenario, but not by others. As we analyze the execution matrix, the result is a decomposition of all of the C2 and sensor functionality necessary, identified by entity. We now build the C2 and sensor functional tables, which describe each functionality against its potential uses, and assigns possible technical implementations. These tables are cross walked with the systems book, and identify what systems should be available to each entity, in order to implement these functionalities. Or if systems are not available to implement these functions, identify the technology gaps. We now have a list of potential systems assigned to the entities the C2 and sensor system profile tables and these two tables together form the basis for the Systems View 4 (SV-4).

5.0 System of Systems Level Analysis

Simulation and Modeling for Acquisition, Requirements and Training (SMART) is defined as "a change in Army business practices, through the exploitation of emerging M&S and other information age technologies, to ensure collaboration and synchronizations of effort across the total Army system life cycle". In our Army studies, we endeavor to achieve the intended objectives of SMART via integrated experimentation , utilizing systems engineering analyses and the representation of C4ISR technologies in models and simulations of varying fidelity. In order to effectively explore C4ISR system of systems concepts, the traditionally fragmented activities of systems engineering analyses, modeling and simulation, and experimentation must be viewed as dependent on one another. These dependencies are reflected in experiment design, data collection, data analysis and in the simulated architecture used for system of systems analyses. This simulated architecture is derived from the data populated in the DoD Framework products to describe the nominal C4ISR architecture. While the scenario was "played out" in as much detail as possible, when performing the systems engineering analyses that resulted in population of the framework products, the complex interactions of these large C4ISR Systems of Systems cannot be predicted easily. To ensure that the architecture can actually support the execution of the chosen scenario, it must be represented in simulation. System of systems simulation environments are needed to study and analyze the complex interactions between the C2, sensor and communications systems, and refine the design to resolve any issues that arise. The DoD uses a number of different simulations systems to do exactly that.

- Constructive combat models such as CASTFOREM. These create, in simulation, friendly and enemy forces and play out their interactions in a simulated battle, without any interactive input from a human operator. They are mainly used to understand interactions in large scenarios with large numbers of entities. At this point they have different levels of fidelity for the C4ISR representation within them, but are continuously being upgraded to included better C4ISR models at higher fidelity. These models are also being enhanced to include multiple-sided opponents, non-combatants, and complex urban structures. Many of them could be modified to provide support for HLS type of scenarios.

- Virtual Simulations. These provide operators with the opportunity to interact with a representation of the world and the threat, and play out scenarios. These simulations are valuable in collecting information about how actual operators would use the C4ISR systems, and with what effectiveness.

- Live Simulations. These are embedded in the actual systems, to provide a training/experimentation mode to analyze the effectiveness of the actual system under certain conditions, and to train the operators in the use of their systems. Operators would use their equipment as usual, but instead of interacting with real signals and threats, they would interact with simulated ones which are stimulating the operators and their real or simulated systems.

6.0 Conclusions

There are still several other aspects of the system that the approach will not cover. The questions of security, limits to access, and the classification of communications and information are serious on many different levels, and require a separate investigation. It is assumed that whoever may need the sensor or intelligence information, and may need to communicate information or intelligence will be able to succeed to the full extent demanded by the mission, whether the mission is considered chronic or acute. However, by having a C4ISR architecture represented in highly detailed computer simulations, the effect of a breakdown in communication and information security, or the loss of sensor coverage can be evaluated, and appropriate means for recovery can be instituted, prior to an actual HLS event.

By laying out the methodology to create a traceability between the results from the simulations of the C4ISR systems, to the C4ISR architecture, to it's intended use highlighted in the execution matrix and the associated operational requirements, creates the basis to easily identify shortfalls, trace it back to the system or systems responsible, and identify whether it was an issue with the technology or with the operational application of the technology. This information can be used to further refine the requirements for future upgrades to the systems, optimize operational techniques and procedures, and modify the systems and their uses so that they can provide the best support within the complex demands of HLS.