Network Science Center
West Point

Advancing the Study of Network Science

United States Military Academy, Network Science Center 2012.12.18

Flowing Valued Information and Cyber-Physical Situational Awareness[1]

By

John James, Frank Mabry, Aaron St. Leger and Kevin Huggins

[1] This interim report for work performed as part of the Flowing Valued Information Project is a publication of the United States Military Academy's Network Science Center. This material is based upon work supported by the U.S. Army Research Office under Grant Award Number MIPR9FDATXR048. The views expressed in this report are those of the author and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, or the Department of Defense.

Contents

Flowing Valued Information and Cyber-Physical Situational Awareness 1

Summary 5

1. Why is information sharing fundamental to Cyber-Physical Situation Awareness? 7

2. Objective 9

3. Modeling complex systems as compositions of components 10

3.1 The Science of Complex System Analysis 10

3.2 An architecture for comparison and incremental construction of complex system models 11

3.3 A network challenge for situation assessment of air defense engagements 13

3.4 A network challenge for situation assessment of the smart grid 18

3.5 A network challenge for situation assessment of command and control 22

4. Can generalizations be made concerning composed complex system models? 26

4.1 A framework for Cyber-Physical Situation Assessment 28

4.2 A Tool for Sharing Protected Information with Selected Users and Groups among Network Nodes ... 31

4.3 Need for Incremental Fielding of Cyber Situational Awareness Capabilities 31

4.4 Cyber Doctrine 32

5. Conclusion 33

Appendix A: An architecture for comparison and incremental construction of complex system models 34

An Early Architecture Analysis Methodology 36

A Distributed, Real-time Architecture Comparison Approach: 37

An approach for comparing alternative distributed, real-time software architectures: 37

References 38

Appendix B: A network challenge for situation assessment of air defense engagements 39

Discussion of the Air Defense Engagement Problem 40

Comparing Architectures for Air Defense Engagement 41

Conclusion 47

References 47

Appendix C: A network challenge for situation assessment of the smart grid 48

Introduction 48

Smart Grid Modeling Methodology 50

Smart Grid Model Simulation 53

Conclusion 56

Acknowledgement 56

References 56

Appendix D: A network challenge for situation assessment of command and control 58

Introduction 58

Organization of the appendix 59

Modeling framework 59

Information Assurance Modeling for Military Systems 66

Information Dominance Modeling 70

A conjecture for resource allocation 70

Summary 72

References 73

Appendix E: Army Common Operating Environment Architecture 74

Appendix F: Seeing the Real World: Sharing Protected Data in Real Time 76

Summary 76

Introduction 76

Formal Extension of the Bell-La Padula result 77

Description of the Existing Service 79

Real-time extensions 83

5. Conclusion 84

6. References 84

Summary

This report summarizes recent results in information sharing and discusses an approach for extending previous results for information architecture understanding and comparison. The report also argues that selective sharing of protected information is fundamental to achieving cyber-physical situation understanding.

The report develops examples of flowing protected information around a central theme that situational awareness for human-in-the-loop control systems already requires cyber-physical estimates on multiple temporal and spatial scales. Thus, issues associated with flowing valued information to create decision-support systems to establish/maintain cyber-physical situation awareness needs to take the reality of broad-based information monitoring and analysis into account. In order to support the "mission command" set of operations (offensive, defensive and stability), the cyber terrain to be considered is necessarily more complex than an understanding of "network topology and node properties". That is, while there are unique properties associated with cyber warfare (e.g. possible speed of execution, possible ambiguity of attribution of malicious activities, distributed nature of execution, and difficulty of identifying associated outcomes), the command decisions concerning use of a cyber weapon or analysis of the effect of enemy use of a cyber weapon will not be based on a consideration of the network topology or node properties but on the physical outcomes estimated to be caused by the cyber weapon. That is, we should consider cyber-physical estimates of outcomes of cyber weapon use. The cyber terrain of interest is the cyber-terrain of communication networks, information networks, and social-cognitive networks (a composite network) whose properties/activities are affected by a cyber event. Then, for a given set of composite networks, the who, what, when where, why and how questions to be answered are those questions associated with facilitating a particular command intent. Selective sharing of protected information is fundamental to these considerations since decision support systems for human-in-the-loop control systems must consider a broad range of cyber-physical situations and cyber-physical outcomes.

Much work remains to be done concerning understanding the dynamics of interaction among the networks of interest for the various domains comprising the cyber-physical terrain of "mission command" operations. For example, we have little or no capability for providing automation support to help solve the "understand the people" problem posed a couple of years ago by MG Flynn. MG Flynn was the intelligence officer (J2) for GEN McCrystal and GEN Petreaus and wrote an article about making intelligence relevant by improving estimates of local preferences and needs.

National efforts in cyber security awareness should include careful and repeated analyses of interdependencies between cyber events, physical outcomes, and cyber approximations of physical outcomes. The evolutionary nature of cyber capabilities is driven by the continuing information systems revolution and necessarily relegates each estimate of the cyber-physical situation as well as the tools, tactics, techniques, and procedures for estimating the cyber-physical situation to a limited interval of temporal-spatial validity. Thus, there is a continuing need for incremental fielding of capabilities for estimating the cyber-physical situation. The approach proposed here for achieving a capability for incremental fielding of tools for estimating the cyber-physical situation is to achieve a science and a framework for objective experimentation and subjective validation of compositions of components

comprising an approximation of the behaviors of the domain of interest. One tool which is described in detail is a tool for selectively sharing protected information among nodes in a distributed architecture. Previous results indicated that each domain of interest will need to be individually understood (i.e. predict future domain states) in order to predict future states of complex systems comprised of compositions of component domains. To realize a current "estimate of the situation" for a domain of interest we can:

1. Begin by identifying a (set of) system invariant(s) which determine component equilibrium points around which system rates of change tend to zero and then proceed to build a set of software architectures for the distributed, real-time problem space by repeatedly:
    - a.1 Identifying the level above which system behavior is to be determined by modifying logical parameters only and partition the problem space (tasks) into appropriate higher-level functional modules using event-based models (i.e. capture the enterprise logical dynamics and compare the logical model behaviors with observed logical behaviors),
    - a.2. Below the level identified in step a.1, partitioning the problem space (tasks) into functional modules, some strictly event-based models, some a mixture of event-based models and differential-algebraic-equation-based models (i.e. capture the enterprise physical dynamics and compare the physical model behaviors with observed physical behaviors).
    - b. Assigning modules to a computational structure (usually pipe and filter computational style), and
    - c. Establishing communication between modules.
2. Choosing a set of quality attributes with which to assess the architectures (pick success criteria),
3. Choosing a set of concrete tasks which test the desired quality attributes, and
4. Evaluating the degree to which each architecture provides support for each task.
5. Returning to step 1.

1. Why is information sharing fundamental to Cyber-Physical Situation Awareness?

The MITRE report on the Science of Cyber Security[2] asserts that '… The "universe" of cyber-security is an artificially constructed environment that is only weakly tied to the physical universe…' The report thus assumes that there are few *a priori* constraints on cyber events which then leads the report to focus on cyber security assessments based principally on cyber events alone. However, that is not the position taken in this report.

While it is certainly the case that cyber events are of primary importance for security assessments of the Internet and other communication networks, and it is furthermore certainly the case that cyber events may be critically important to the proper operation of many, if not all, critical infrastructures, it is also certainly the case that cyber events and cyber outcomes are not the most important events and outcomes associated with critical infrastructures. Indeed, the position taken here is that cyber outcomes of national-level interest (both security-related outcomes and non-security-related outcomes) are necessarily grounded in the physical universe since it is precisely the physical outcomes which are considered most important (e.g. while determining whether a smart grid information server has been hacked is certainly important, the principle outcome of interest for power system operators is whether power is being generated and delivered as expected and secondarily whether a hacked smart grid server offers a threat to the generation and distribution of power and thirdly whether a hacked smart grid server offers a threat to one or more other critical infrastructures). Moreover, it is the dependence of physical outcomes on cyber events which is in a period of rapid change and the nature and extent of interdependencies between physical and cyber systems is thus of pressing interest to cyberspace situation assessment efforts. It is also the case that the most accurate models of the propagation of cyber events throughout interconnected networks of devices, applications and people are necessarily compositions of cyber-based models (i.e. discrete time and space models) and physics-based models (i.e. continuous time and space models).

Furthermore, without directly relating cyber events to physical outcomes, it is very easy to create situational assessments which are physically impossible (e.g. if the point of origin of an event and associated time delays required for propagation of effects throughout an enterprise are not accurately understood, then decision makers may be led to believe that that outcomes which may actually occur in the future have already occurred and falsely assume that potential remedial actions are not an option). For instance, one false assumption sometimes associated with deliberate or inadvertent cyber events is that cyber events and their effects are instantaneous. However, while local propagation of cyber event occurrences and subsequent effects are often almost instantaneous, the physical constraints of real (causal) systems impose some finite propagation delay (latency) associated with cyber events and their effects. In addition, for large-scale, distributed systems, the propagation delays (latencies) are often far from instantaneous. For example, the amount of time required to disconnect Egypt from the Internet was about

[2] MITRE, "**Science of Cyber-Security,**" Report JSR-10-102, The MITRE Corporation JASON Program Office 7515 Colshire Drive McLean, Virginia 22102, November 2010, , page 1. Downloaded on November 28 20110 from: http://www.nitrd.gov/fileupload/files/JSR10102Science_of_cyber20101128.pdf

a half-hour and the lead time associated with propagation of the last major cascading failure of the power grid in the United States was about a half-hour.

For decades the Department of Defense has recognized the operational impacts, indeed the disruptive effects, of the ongoing information systems revolution on weapons capabilities and on the command and control of joint and coalition forces. More recently, the effects of the information systems revolution on political, social, economic, and cultural changes across the globe have become apparent. We currently have no means for objectively assessing (predicting) the outcomes, or the rate of change of the outcomes, for which the information systems revolution will continue to alter relative military capabilities for offensive, defensive, and stability operations or associated changes in political, social, economic, and cultural interdependencies across the globe. Without a capability for assessing current changes due to the continuing information systems revolution, we will not be able to improve the security of cyberspace since our models of systems dynamics will be faulty and will lead to system failures and subsequent exploitation of those failures. The White House recently released the strategic plan for the federal cybersecurity research and development program[3] which outlines the national plan for achieving a trustworthy cyberspace. One focus area of this plan aims to achieve a "deep understanding of cyberspace." As part of the effort to achieve a deep understanding of cyberspace, the plan asserts that "Actions in cyberspace are instantaneous…"[4] and declares that if we are to "… manage our moving target capabilities effectively and instantaneously…" then "…we must greatly enhance our ability to monitor, model, analyze, and understand our own system, the systems in cyberspace with which it interacts, and the threat environment at that point in time." The majority of this report is devoted to discussing development of a capability for monitoring, analyzing, and understanding present and future states of cyber-physical domains of interest. In this report, we attempt to clarify the relationships between actions and the effects of actions, especially for the case of human-in-the-loop feedback control systems in which there is always some propagation delay that occurs between a control action being taken and the effect of that control action being propagated throughout the system under control. In case of feedback control systems, effects are **no**t instantaneous and, in many cases, increasing the latency associated with control action propagation may cause the controlled system to become unstable.

Improved Internet-scale anomaly detection tools are required for closing the gap between current processes and tools for ***cyber situational awareness*** and current decision support capabilities for ***cyber operations***. However, improved *anomaly detection and visualization tools alone are* ***insufficient*** for closing the capabilities gap between awareness and decision. Indeed, we observe here that *cyber-physical awareness* and *cyber-physical decision-making* ***dominate*** the challenges associated with closing the gap between cyber awareness and cyber operational decision-making. That is, since all of the outcomes of interest (e.g. the state of political, military, economic, social, infrastructure, and information systems) exist

[3] Executive Office of the President, **Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program**, http://www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf

[4] Ibid, page 9.

in the physical realm, the cyberspace "pale image of reality" which approximates the "real world" must itself be continually questioned and adjusted to be "close enough" for making decisions concerning the effects of cyber events on physical outcomes. For instance, consider the recent anomaly of essentially disconnecting Egypt from the Internet. Such an event was previously considered almost impossible to achieve (there is no Internet "off switch"). However, the disconnection of Egypt from the Internet in less than an hour proved to be feasible not only because of the few logical connections which had to be interrupted (the logical network visualization of the Internet), but also because those logical connections were positioned on communications devices which were in close proximity to each other (the physical network visualization of the Internet) and were administered by a small group of people under the control of the government (the social/cognitive network view of the Internet). We currently have only very limited capability to understand (predict) and visualize whether similar junctures of logical, physical, and social networks exist which might enable decisions to achieve local/national/regional Internet disruptions similar to that which occurred in Egypt. Some questions which need to be reliably and continuously answered include:

- Is the Internet (or pick a network) working properly?
- What are the critical juncture points of composite network (e.g. compositions of logical, physical, and social networks) overlaps/interconnections/interdependencies?
- Are these critical juncture points operating properly?
- How are these critical juncture points evolving over time (e.g. how are the sets of logical/physical/social network junctures evolving over time)?
- Are more critical junctures being created?
- What are the political, military, economic, social, infrastructure, and information network system implications of disruption of these critical juncture points both by level within a region as well as by region?
- How do we visualize the critical junctures, visualize their evolutions over time and visualize the impacts of juncture disruption?
- How do we estimate how those changes in critical juncture dynamics and information flow affect the achievement of national goals (e.g. political goals, military goals, economic goals, social goals, infrastructure goals, information goals, …)? And
- Do cyber capabilities exist (or are they being developed?) to implement the doctrinal ideas for ***cyber strategic deception*** and ***cyber strategic surprise*** summarized in the "net force maneuver[5]" discussions of a few years ago?

2. Objective

We cannot achieve a trustworthy cyberspace if we cannot understand (predict) expected outcomes for entities of interest and assess whether systems are functioning as expected. In that regard, the objective of this report is to outline an architecture for incremental construction and update of complex system models

[5] C. Hunt, J. Bowes, and D. Gardner **Net Force Maneuver,** Proceedings of the 2005 IEEE Workshop on Information Assurance, West Point, NY. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1495982&userType=inst

as compositions of component system models. Several examples of applying the approach are sketched out in which a more precise understanding of the changes in complex systems comprised of compositions of cyber systems components and physical systems components is made possible through explicitly capturing the nature of the interdependencies between cyber and physical models.

The next section begins with a statement of scientific challenges in understanding cybersecurity and follows with a presentation of an architecture comparison approach as a means of incrementally discovering and updating an explicit understanding of cyber-physical system current state and the evolution of the cyber-physical system state over time. This is followed by several examples concerning the kinds of cyber and physical interdependencies which can be explicitly modeled for large scale systems and some results possible from considering such composed models. The examples include air defense target engagement, power system control, and military command and control. In addition, a short section is provided which attempts to generalize results from the examples in terms of improving understanding of the impacts of cyber events on the behavior and evolution of critical infrastructure states. After deliberating on the discussion below, it is hoped that readers will agree that the most accurate estimates of a cyber-physical security situation are necessarily based upon "a little of this" from the set of discrete (cyber-based) models and a "little of that" from the set of continuous (physics-based) models.

3. Modeling complex systems as compositions of components

3.1 The Science of Complex System Analysis

The White House trustworthy cyberspace strategic plan referenced above outlines the national level intent for "Developing an organized, cohesive scientific foundation to the body of knowledge that informs the field of cybersecurity through adoption of a systematic, rigorous, and disciplined scientific approach."[6] This section describes extensions to a previously-developed systematic and rigorous approach for understanding the behaviors of complex, distributed systems through construction and analysis of system architectures consisting of compositions of component models. The section also reviews application of this architecture understanding approach to several complex systems. This approach is based on the repeated application of the scientific method by the recurring sequence of: (1) application of known laws of physics (model behaviors in the vicinity of fixed points) to partition the problem space,(2) hypothesis generation (model generation from data describing dynamical behaviors of components resulting from the partitioning), (3) repeatable experiment design and implementation (model implementation and execution), (4) hypothesis confirmation/denial (objective verification against measured data) via model predicted behaviors matching/deviating from observed behaviors, and (5) hypothesis validation by human decision makers concerning the viability (subjective estimates of the virtual prediction matching measured reality being "close enough") of the model to assist in decision-making activities associated with achieving desired enterprise behaviors.

[6] Executive Office of the President, **Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program**, page 3.

3.2 An architecture for comparison and incremental construction of complex system models

Large-scale, distributed systems (e.g. power generation and distribution systems, factory control, communication networks, distributed simulation networks, military command and control systems) have been growing in size and complexity. Tools and techniques for analysis of these systems have also been changing. One approach for dealing with the growing size and complexity of distributed systems has been to improve techniques for partitioning the problem into sub-problems and arranging these system components into a system architecture.

Appendix A[7] provides some background information and additional details concerning partitioning a given system into components which can be subsequently composed to approximate the behaviors of the domain of interest. As discussed in Appendix A, for the domain of distributed real-time systems, communication is an integral member of the problem space and must be explicitly considered. Establishing communication between modules should be a step in the architecture development process, equal with partitioning the problem space and assigning functional modules to a structure. Appendix A also asserts that a functional partitioning of a given enterprise domain will normally result in components whose internal state depends only on the previous state and current inputs (i.e. component dynamics are independent of each other).

The component independence assumption is true much of the time for those components supporting higher-level decisions leading to engagement events, especially force operations decisions which set the environment for use of deadly force. However, the component independence assumption is almost never true for modeling lower-level physical processes, such as aircraft and missile guidance control, sensor control, and control of engagement processes, all of which are integral processes of the distributed, real-time problem space. Stated another way, for many physical processes including planning and conduct of military operations, the failure of the independence assumption for distributed, real-time components arises from the fact that the distributed nature of motion in the domain of interest (e.g. for military operations the battlespace state for engagement decisions is constrained by the location and movement of friendly and enemy ships, missiles, aircraft, tanks, helicopters, troops, …) means that very high-level decisions can result in producing constraints which dramatically change the operational environment for low-level components. The low-level components then quickly produce different outputs which change the state of the higher-level components inside their decision cycle (i.e. the component independence assumption is invalid because we have feedback loops among components comprising a mixed-signal, or hybrid, problem space with interdependent components).

[7] The architecture comparison approach outlined here is a modification of the one reported in J. James and R. McClain "Tools and Techniques for Evaluating Control Architecture," **Proceedings of the 1999 IEEE International Symposium on Computer Aided Control System Design**, Kohala Coast, HI , USA, August 22-27, 1999, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=808706

Similarly, for critical infrastructure processes complex feedback processes between high-level decisions and low-level system dynamics can often invalidate an assumption of component independence. For example, for the case of power system dynamics, an assumption that the power generation and distribution system is in a state of equilibrium for changes in frequency ignores the fact that smart grid implementation will enable use of explicit frequency control components (e.g. "wide area control" based on use of synchrophasor data to respond to deviations in frequency between synchronous generation and distribution areas due to changes in demand). That is, there exists a feedback loop between synchronous areas which enables control to synchronize the frequency at 60 Hz among a set of largely independent (but not totally independent) power generation and distribution areas.

A Distributed, Real-time Architecture Comparison Approach:

While functional segmentation is a natural approach to follow in construction of software modules (since implemented functionality of software process models and data schema can be directly related to user functional requirements), the functional partitioning of components may not be the best approach for architecture development. An architectural comparison approach is thus required. The relative ability of alternative software, hardware and communications architectures to react to expected failure modes will be determined by the detailed partitioning of required operations into functional modules, the mapping of resulting distributed software processes onto the distributed computation and communication resources, and the execution of combined system functionality across components which may be widely distributed in space and time. Recent interest in network science supports consideration of components which comprise a network of communication devices (primarily a hardware layer), components which comprise a network of application components (primarily a software layer), and components which comprise a social network of individuals collectively involved in the domain under review.

An approach for comparing alternative distributed, real-time software architectures:

1. Begin by identifying a (set of) system invariant(s) which determine component equilibrium points around which system rates of change tend to zero and then proceed to build a set of software architectures for the distributed, real-time problem space by repeatedly:

    a.1 Identifying the level above which system behavior is to be determined by modifying logical parameters only and partition the problem space (tasks) into appropriate higher-level functional modules using event-based models (i.e. capture the enterprise logical dynamics and compare the logical model behaviors with observed logical behaviors),

    a.2. Below the level identified in step a.1, partitioning the problem space (tasks) into functional modules, some strictly event-based models, some a mixture of event-based models and differential-algebraic-equation-based models (i.e. capture the enterprise physical dynamics and compare the physical model behaviors with observed physical behaviors).

    b. Assigning modules to a computational structure (usually pipe and filter computational style), and

c. Establishing communication between modules.

2. Choosing a set of quality attributes with which to assess the architectures (pick success criteria),
3. Choosing a set of concrete tasks which test the desired quality attributes, and
4. Evaluating the degree to which each architecture provides support for each task.
5. Returning to step 1.

3.3 A network challenge for situation assessment of air defense engagements

The first example of applying the architecture comparison approach described above is the domain of air defense engagements. While command and control of military operations is a group decision-making process (i.e. social network process) which can take many months for national-level coalition operations, target engagement is a rapid reaction group decision making process organized as a combat crew drill. Cyber event responses are similar in cognitive complexity and time constraints to combat crew drills.

Air defense command and control usually places airborne entities into one of three categories, friendly, enemy, or unknown. In the past, air defense engagements have resulted in a number of events in which friendly aircraft or civilian aircraft were mistaken for hostile targets and destroyed. A continuing effort of situation assessment for air defense engagements is to comply with the laws of land warfare for engaging aircraft with hostile fires. While self defense is always a reason for engaging hostile aircraft, engaging potential targets after receiving fire is an attempt to extract revenge while engaging hostile threats before they destroy their intended targets is an attempt to protect valuable assets. Thus, a key element of air defense engagements is to assess the situation in terms of the relative level of hostilities among potential combatants and the norms of airspace use in order to determine if a potential target should be engaged prior to the target releasing a weapon. This section will not cover the various means for developing the Rules of Engagement (RoE) but simply observe that as the RoE become less restrictive the probabilities of mistakenly engaging friendly aircraft or non-combatant aircraft increase and also note that one of the constraints on network information systems is to both (1) rapidly and reliably identify non-combatant, friendly, and hostile targets and also (2) rapidly share changes to the RoE as the situation develops.

A consistent issue in conceiving, designing, and constructing computer-controlled systems is achieving adequate models of system components and determining which components are independent of other components or the nature of interdependencies between components. The arrangement of relationships between dependent and independent components is then used to determine the system architecture. Modification of the behavior of the network of components comprising the system architecture is the central task of control engineering. Classical design approaches focus on single-variable and multivariable components whose dynamical models are independent of each other. However, interest in discrete-event dynamical systems and the growth of hybrid systems tools and techniques has created the need to evaluate event-based components as well as components whose models include both discrete logic and continuously evolving variables. The mixed-signal issues of hybrid systems analytical problems have been encountered repeatedly in the field of artificial intelligence as the “pixel-to-predicate” problem for vision understanding or the “sensor-to-shooter” problem for military applications. An Internal Research and Development (IRAD) effort at Lockheed Advanced Technology Laboratories was conducted a number of years ago to develop an approach for evaluation of alternative architectures for control of large-scale,

networked systems whose components may or may not be independent and whose activities are distributed in time and space. The project evaluated alternative architectures for control of large-scale, distributed systems as well as conducted an analysis of approaches for recovery from various system failure modes. The material provided here is based upon a paper which summarized project results and was presented at a technical conference[8]. The fundamental man-in-the-loop decision cycle for ballistic missile air defense engagements associated with events which occur from the time of a Ballistic Missile threat launch through the time of intercept and assessment of engagement outcomes to determine whether the target must be re-engaged is depicted in Figure 1 below.

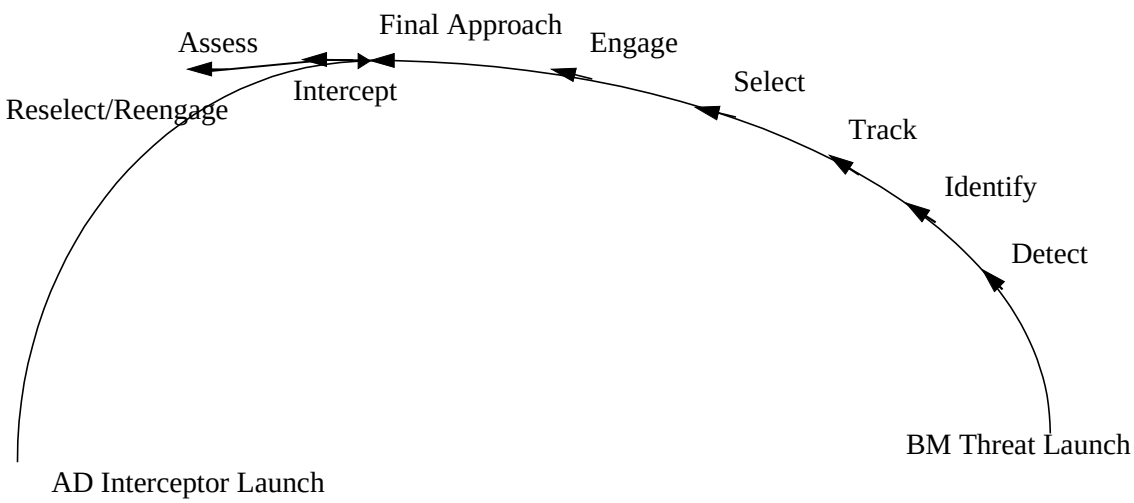


Figure 1. Ballistic Missile Engagement Sequence

Comparing Architectures for Air Defense Engagement

A comparison of Engagement Operations architectures for air defense operations was conducted during an Internal Research and Development (IRAD) project. That project evaluated alternative approaches for providing air defense of maneuver forces for missile (ballistic and cruise missiles) and air-breathing (fixed-wing and rotary-wing) threats. The project involved modifying the Extended Air Defense Simulation (EADSIM) program to support architecture analysis. EADSIM is a high-fidelity (about 500,000 lines of C and Fortran code) program which models the logic and dynamics of air-defense engagement processes. The statement that the architecture analysis approach begins with identifying system fixed points (system invariants) is a new assertion. This was an assumed condition for the air defense engagement process since persistent models of system dynamics are in fact constructed around system fixed points. The top-level

[8] The air defense engagement process partitioning problem presented here is a modification of the one reported in J. James and R. McClain "Tools and Techniques for Evaluating Control Architecture," **Proceedings of the 1999 IEEE International Symposium on Computer Aided Control System Design**, Kohala Coast, HI , USA, August 22-27, 1999, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=808706

fixed point for the engagement process logical model is the invariance over the time and space of a given engagement of the intent to provide protection of assigned assets subject to the laws of land warfare (i.e. engage hostile aircraft and missiles in accordance with the Rules of Engagement as discussed above). The top-level fixed points for the target and the engagement vehicles is the invariance over the time and space of a given engagement of the compliance of the vehicle position, velocity and acceleration dynamics with the laws of physics. The Extended Air Defense Simulation (EADSIM) simulation system used in the project complies with logical and physical (hybrid) constraints and was constructed over a number of years to enable investigations of alternative solutions to air defense engagements.

Step 1a: Partition the Engagement Operations Problem Space:

While the Corps air defense problem is a very large one, resource constraints led us to restrict ourselves to a subset of the problem space. Specifically, we were not able to examine in detail the continuous systems modeling components of the Extended Air Defense Simulation (EADSIM) (flight, sensor and propagation processes) but have studied the Flexible Commander logic implementation within the command and control logical process. The EADSIM solution is a strictly hierarchical one (as opposed to a more flexible netted, distributed one) where each commander deconflicts feasible engagements for subordinates and assigns targets to each assigned weapon system.

In this context, our consideration of the Architecture Analysis Methodology (AAM) problem space is restricted to the engagement sequence of Engagement Operations summarized in Figure 1. Interrupting the EADSIM logical simulation process supports simulating alternative architectural approaches to implementing software support to engagement operations. Modules for detection, identification, tracking, selection (allocation), engagement, final approach, engagement assessment, and disengagement or reengagement or new target processes could be implemented. Modules for detection and identification would naturally be concentrated in the unit sensor systems but synchronization with other systems (especially coalition partner and national technical means) require portions of the functionality to be distributed. The sensor fusion problem becomes more complicated as we increase the number of sensor (radar) inputs being integrated locally. Similarly, the tracking problem also becomes harder as track results from local fusion processes must be resolved with more tracks from remote sensor systems. We have implemented a modification to EADSIM which extends engagement logic (the Flexible Commander module) code to support a netted, distributed (cooperative) approach to target deconfliction (see Figure 1).

The system architecture must meet system requirements for successful completion of the engagement sequence of Figure 1 under both nominal conditions and stressed conditions (failure modes). Figure 1 reflects the mixed-signal nature of the problem in depicting the engagement events (which are states in the set of engagement states for each target engaged by each unit) and paths of threat and interceptor missiles (which are represented as sequences of points in four-dimensional space of range, azimuth, elevation and time with respect to each sensor which tracks the motion of each missile). An implementation would be comprised of a hardware architecture, a communication architecture and a software architecture. For purposes of the software architecture comparison we assumed that the hardware and communications architectures were given and proceeded to develop a framework for comparing alternative software architectures.

Step 1b: Assign functional modules to computational structure:

While recognizing that the optimal solution of the target engagement problem is a mixed-signal problem, we restricted our investigation of alternative architecture solutions to implementation of logical components using EADSIM and relied on the unmodified evolution models of EADSIM to model the flight, sensor and propagation processes and provide the values of the evolution variables at the update intervals of the decision logic.

Step 1c: Establish Communication Between Modules:

Alternative software architecture styles include: Main/Subroutine, layered (distributed), data abstraction (object-oriented), pipe & filter, repository (blackboard), and event-based (implicit invocation of procedures). The software architecture will probably be required to work with many different hardware architecture configurations, including different numbers of major components. It is expected that alternative hardware choices, such as increases in numbers of sensors or in the number of command and control nodes or alternative functional allocation between sensors, command and control nodes and missiles would require alternative communication capability between system components but these alternatives were not modeled in this effort.

We depended upon EADSIM to simulate communication between other modules. While we expect that different architectural styles will cause different impacts on the communications, without additional modeling of communication details, tradeoffs between architectural communication approaches cannot be analyzed.

Step 2: Choose a set of quality attributes:

The attributes chosen for this project were (1) relative ability to reconstitute the defense and (2) relative ability to engage air defense threats.

Step 3: Choose a set of tasks:

The tasks chosen for this project were (1) time required to reconstitute the defense (effectiveness of the reconstituted defense (3) relative lethality of the defense (number of air breathing threats and theater missile threats before "leakage"), and (4) relative ability to avoid fratricide.

Step 4: Evaluate the degree with which alternative architectures support the tasks:

The modifications to EADSIM were implemented to support comparing a netted, distributed command and control architecture to four other command and control architectures: 2-tier centralized, 1-tier centralized, autonomous tactical operations centers and autonomous surface to air missile batteries. A series of performance cases were run against a total of five architectures to determine the effectiveness and efficiency of each under a range of stressing cases. The five architectures compared were: centralized command with two tiers of command, single tier centralized command, autonomous Tactical Operations Centers (TOCs), autonomous Surface-to-Air Missiles (SAMs), and the new coordinated structure using a nearest neighbor coordination algorithm. The netted architecture was setup to coordinate TOCS at the same command tier (peer-to-peer). We measured both effectiveness (the percentage of targets killed) and

efficiency (number of kills per missile) of each architecture to provide a more complete measure of the overall systems utility than simply measuring kills.

Step 5: Return to step 1

Common Details in the Testing Scenario: Five alternative C3I architectures were implemented and compared by evaluating the performance of each one against an identical series of missile attacks of increasing intensity. Each architecture defended 3 point assets. Each architecture had equivalent defensive fire power at its disposal: 4 surface-to-air missile (SAM) units consisting of a radar and launcher combination. The fire unit behaviors were implemented with a Flexible SAM ruleset. Results of an analysis of one architecture for command and control of air defense engagements is shown in Figure 2. Multiple alternative architectures for air defense engagements were analyzed and compared.

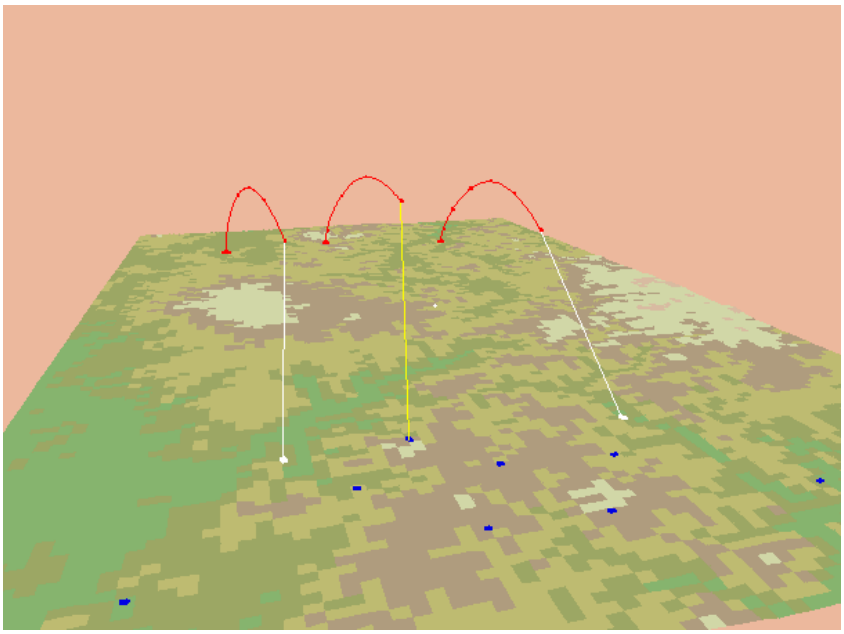


Figure 2. EADSIM 3-Dimensional Output

The logical and physical simulation outcomes are clearly evident in Figure 2. The goal of the target deconfliction logical dynamics was to reach a feasible solution to the “you take that one, I have this one” problem of which air defense asset engages which target prior to engagements no longer being feasible to protect assigned assets. The goal of the air defense dynamical solution was to calculate a feasible solution for guiding each air defense missile to a predicted intercept point based on ballistic missile trajectories. For the three ballistic missile targets, the outcomes of the logical system dynamics was to allocate three of the four air defense assets to each engage one of the targets and the outcomes of the physical system dynamics was to provide tracks of three ballistic missiles from launch to interception and to provide tracks of three air defense missiles from launch to interception. By repeatedly altering the logical system constraints concerning how the target allocation problem was to be resolved, the simulation system was configured to enable evaluation of alternative command and control architectures for relative effectiveness

(value) in achieving protection of assigned assets from hostile ballistic missile fires. The explicit inclusion of communication systems among distributed air defense units as part of the evaluation architecture also enabled consideration of the effects of cyber events on the conduct of air defense engagements. However, this capability was not investigated in the project.

3.4 A network challenge for situation assessment of the smart grid

A central challenge in hybrid system control is the fact that even though it has been mathematically shown that solutions exist to the composed problem (compositions of discrete constraints on system evolution and continuous constraints on system evolution) constructive approaches for building solutions to the composed problem have yet to be discovered. An early attempt to explicitly include notions of time in simulations and implementations of mixed-mode systems was the Signal language developed in France[9]. However, the Signal language[10] has had continuing issues with combinatorial explosion in constructing solutions to combining discrete and continuous simulation tasks.

Comparing Architectures for situation assessment of the smart grid

The majority of the section has been taken from a paper prepared with Dr. Aaron St Leger as part of a project sponsored by the Defense Threat Reduction Agency (DTRA) and co-authored by Dr. Dean Frederick.[11] The Network Science Center is beginning the second year of a three-year project to investigate the effects of weapons of mass destruction (WMD) on the smart grid. An initial model of a few of the major smart grid components have been built using the Matlab/Simulink set of tools. Details of initial results are provided in Appendix C. This section discusses the proposed framework for comparison of alternative smart grid architectures and discusses how the flexible nature of the Matlab/Simulink toolset enables (1) evaluation of alternative smart grid architectures, (2) comparison of alternative hypotheses concerning WMD effects on smart grid dynamics, (3) Sharing of models and results with other research and development projects seeking to understand smart grid dynamics, (4) potential for transition of results to practice since Matlab/Simulink is the world's most widely used platform for control system design and implementation.

Step 1a: Partition situation assessment of the smart grid problem space:

Developing a suitable model for smart grid simulation is challenging as the smart grid is still emerging and evolving as technology and control techniques continue to improve. The modeling methodology presented here is developed in a flexible fashion to allow for implementation of new technology and control schemes.

---

[9] E. Rutten and P. Le Guernic, Sequencing data flow tasks in SIGNAL, http://hal.inria.fr/inria-00074552/en/

[10] M. Pouzet and R. Pascal, Modular Static Scheduling of Synchronous Data-flow Networks: An efficient symbolic representation, http://www.di.ens.fr/~pouzet/bib/emsoft09.pdf

[11] A. St. Leger, J. James, and D. Frederick, Modeling Smart Grids as a Set of Composite Networks, submitted for publication.

Flowing Valued Information and Cyber-Physical Situation Awareness

The smart grid as defined by the National Institute of Standards and Technology (NIST), shown in Figure 3, was used as a starting point for modeling.

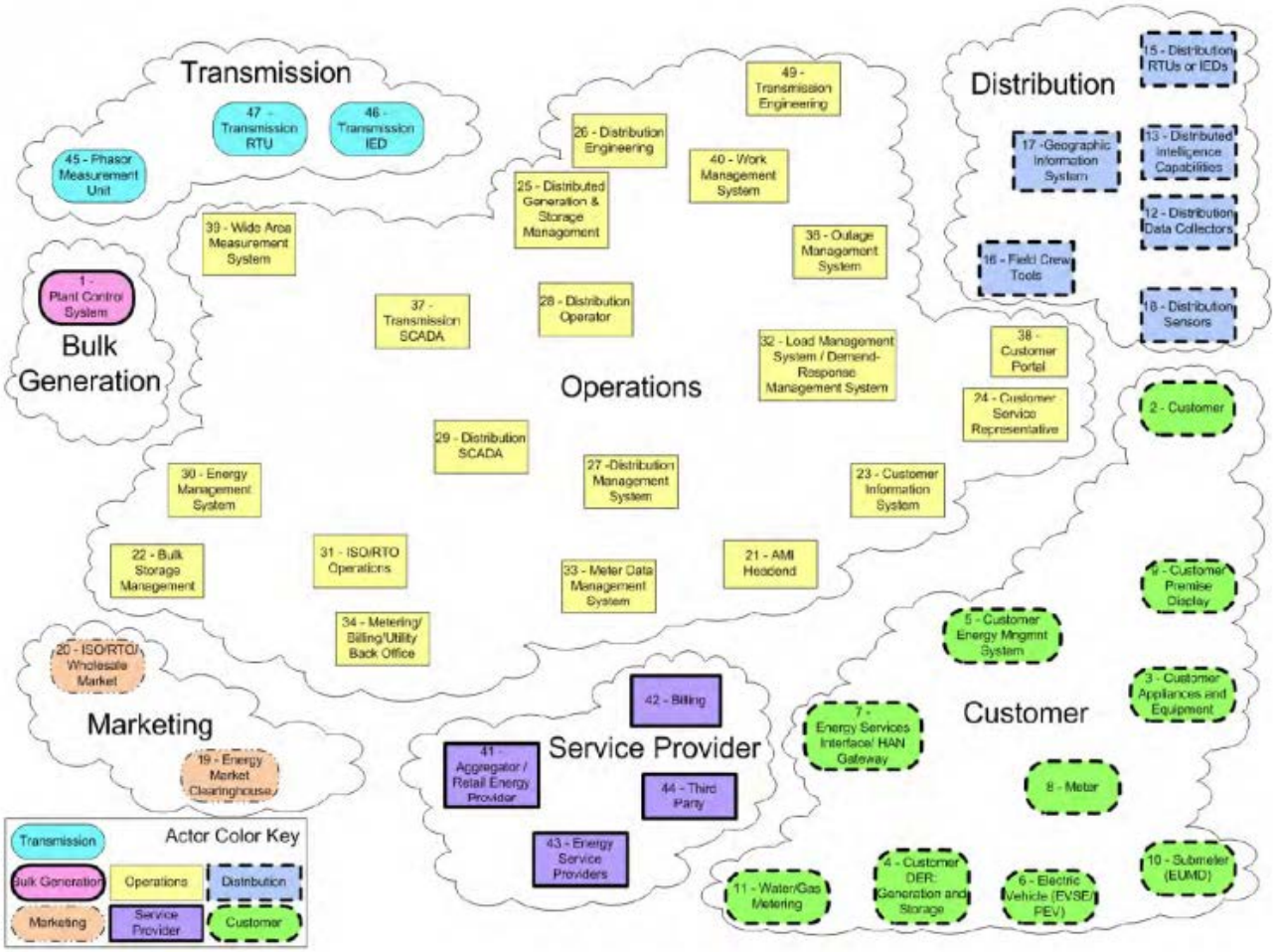


Fig. 3 Actors in the Seven Domains of the Smart Grid

As noted above, the step in architecture comparison recently added to the architecture comparison methodology is to first identify the fixed points (invariant conditions) around which the architecture components can be safely assumed to be stationary (non-time-varying) over the course of the modeling and simulation application period. For the case of the smart grid, the existence of the national-level synchronous machine which comprises the power grid means that the primary physical system invariant constraint is the condition for operation of the grid at a frequency of 60 cycles per second (Hertz). Of course, one of the goals of the modeling and simulation effort is to precisely identify those system components and feedback loops which maintain (control) the frequency of operation at 60 Hz and experiment with those effects which might cause the frequency to vary enough to significantly affect the proper operation of the grid. A logical invariant condition (fixed point) is that the grid operates at a profit for the participating individuals and corporations (i.e. homeowners will “opt in” to smart grid operational constraints to save money and corporations will “opt in” to increase profits). The system architecture must meet system requirements for successful completion of the power system enterprise process interactions

summarized in Figure 3 under both nominal conditions and stressed conditions (failure modes). Figure 3 reflects the discrete-event signal nature of the problem in depicting the logical partitioning of smart grid activities. The Bulk Generation processes as well as the Transmission processes and Distribution processes represented in Figure 3 are in fact constrained by the physics of electrical power general and distribution so the component models of these processes are necessarily mixed-signal (or hybrid control) processes. An implementation of the smart grid will be comprised of a hardware architecture, a communication architecture (communication network) and a software architecture (application network). The smart grid will be controlled at the top level by the various control systems with humans-in-the-loop (social networks) operated by local utilities and Independent System Operators (ISOs). The 60 Hz invariance constraint has proven to be "close enough" for reliable operation of the power grid. However, an example of the dependence of the frequency associated with power generation and distribution on other events which change demand is shown in Figure 4[12]. The variability of the frequency at a faster resolution demonstrates the need for frequency control. We seek to understand frequency variability to investigate wide-area control of the smart grid and possible effects of WMD/cyber events on stable operation of the smart grid.

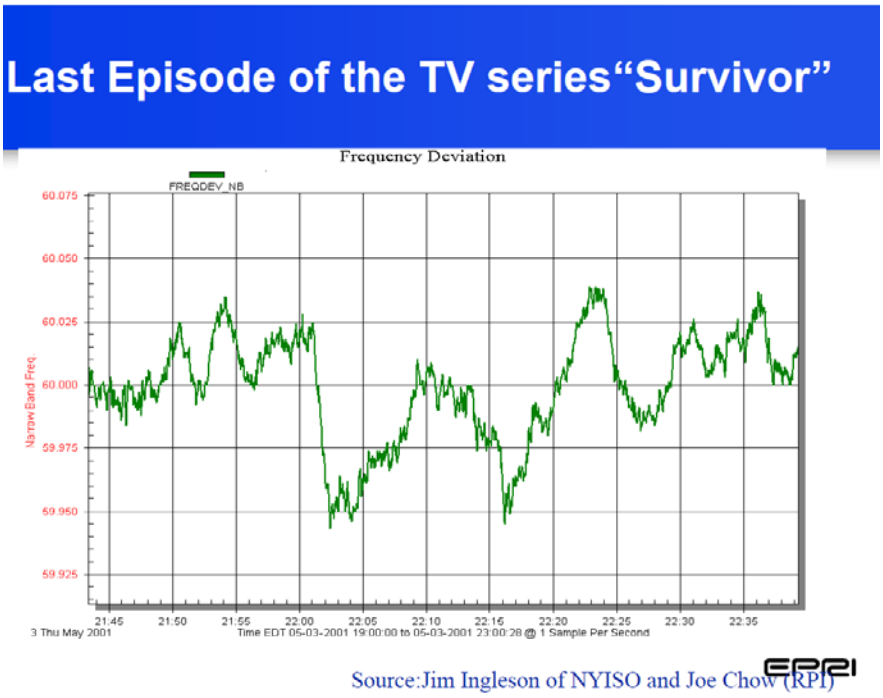


Figure 4. Local frequency variability of the power grid

The last episode of the TV series "Survivor" began at 10PM (22:00 hours) and, as indicated by the data in the figure above, the frequency dipped almost a tenth of a cycle per second in less than three minutes (from about 60.025 cycles per second to less than 59.950 cycles per second). It then took over 7 minutes to return the frequency to 60 HZ. The data shows the effects of large changes in demand (when a

[12] Downloaded from http://central.tli.umn.edu/PrecursorToCatastrophe.pdf on 15 December 2011.

lot of TVs were turned on to start watching the show) on the frequency of the power generated. Control decisions by humans in power generation and control centers are made today based upon projections of power flow assuming sinusoidal steady state generation and distribution of power (i.e. a straight line of 60HZ over time instead of the variability around 60 HZ observed in the figure above). Control engineers working in the power generation and control facilities know that the assumption is not entirely accurate but they also know that it is normally "close enough." However, they also know that the assumption is not "close enough" in the event of a cascading failure of power generation and distribution components. It may also be that case (yet to be encountered) that a cascading power failure situation may be created by manipulation of decision support data being made available to "humans-in-the-loop."

Step 1b: Assign functional modules to computational structure:

We initially experimented with the SimPowerSystems[13] extension to the Simulink tool since this enables direct construction of hybrid system models by linking the discrete-eventsimulation capabilities of Simulink with the continuous-time simulation capabilities of Matlab. However, it turns out that the lower-level files which define the details of the continuous-time simulations are not available as source files for extension by research and development projects. Thus, a decision has been made to extend the Power System Toolbox[14]. This toolbox is based on Matlab files which are available for modification. We will explicitly compose the Power System Toolbox Matlab files into modules which can be executed as Simulink modules which comply with hybrid constraints. Details are provided in Appendix C.

Step 1c: Establish Communication Between Modules:

Alternative communication architectures continue to be discussed and constructed[15] where the use of power line communication components and Internet or intranet communication components are frequently mentioned. Alternative software architecture styles include: Main/Subroutine, layered (distributed), data abstraction (object-oriented), pipe & filter, repository (blackboard), and event-based (implicit invocation of procedures). The software architecture will probably be required to work with many different hardware architecture configurations, including different numbers of major components.

We are explicitly modeling communication components using Matlab/Simulink since we anticipate that a number of the failure modes of the smart grid will include those associated with failure of communication components. Details are provided in Appendix C.

Step 2: Choose a set of quality attributes:

Since our project is focused on understanding the effects of weapons of mass destruction (WMD) on the smart grid the quality attributes are those which measure the performance of the smart grid due to

---

[13] http://www.mathworks.com/products/simpower/

[14] http://www.mathworks.com/matlabcentral/linkexchange/links/86-power-system-toolbox

[15] http://www.comsoc.org/Smart-Grid

anomalous conditions. We have initially chosen to explicitly measure power flow and current and voltage values over time in response to step changes in component conditions.

Step 3: Choose a set of tasks:

The tasks chosen for the architecture is to enable implementation of the smart grid. The definition of smart grid capabilities are those defined by the National Institute of Standards and Technology and details are provided in Appendix C. Our project is explicitly focused on understanding smart grid failure modes due to WMD effects so our architecture choices are made with a view towards making clear those failures which are due to logical errors (logical failure modes) and those which are due to physical dynamics of the smart grid (continuous system failure modes).

Step 4: Evaluate the degree with which alternative architectures support the tasks:

The Matlab/Simulink models allow for rigorous system modeling and simulation and construction of repeatable experiments from system models and system input data sets. Initial results for results which match those from existing models is discussed in Appendix C. Initial results indicate that the approach does enable incremental construction of smart grid models which can be verified against data sets under construction (e.g. the synchrophasor data base[16]).

For the problem of evaluating the potential effects of WMD on the smart grid, it is expected that different potential effects will have dramatically different effects on smart grid dynamics. For example, an electromagnetic pulse (EMP) which is estimated to cover a wide area will have a set of consequences that are very different than the set of consequences due to an explosion at a critical juncture of communication network capabilities and information network capabilities. It may be the case that an architecture implementation that is more capable against an EMP event may be less capable against an explosion event.

Step 5: Return to step 1

The smart grid project is just beginning the second year of a three year effort. We expect to make the models and data sets used in the project available on the web for other researchers to repeat our results and, if interested, expand the models and architectures under investigation.

3.5 A network challenge for situation assessment of command and control

The first computer system involved in decision support for command and control was part of the Semi-Automatic Ground Environment (SAGE) [17][18]. SAGE was the first large-scale distributed information system. SAGE became operational in 1963 and remained operational into the 1980s in the United States and in Europe. The system involved numerous humans-in-the-loop to operate and, although it was never used in wartime, enabled air defense of North America and Europe. Today, command and control systems are

[16] www.nerc.com/docs/oc/rapirtf/RAPIR%20final%20101710.pdf

[17] http://www.ibm.com/ibm100/us/en/icons/sage/

[18] http://www.computermuseum.li/Testpage/IBM-SAGE-computer.htm

present from the lowest tactical level to the highest strategic levels but the capabilities of these systems remain those supported by the first command and control system: situation awareness for command decisions and assignment/control of forces allocated to meet command intent. A current command and control system under development for the Army is the Joint Battle Command Platform (J-BCP)[19]. The joint battle command platform may be implemented on a smart phone and have the ability and authority to access the Internet.

Comparing Architectures for situation assessment of command and control

As indicated in the earlier two examples of incremental architecture comparison, the initial choices to be made are the system invariant(s) associated with implementation and execution of the architecture. For the case of military command and control, the only system invariant known to the author is command intent. That is, every variable or constraint of interest other than command intent that is associated with military operations is subject to change over the course of an operation. General Eisenhower stated this situation as: "Plans are nothing; planning is everything[20]." That is, all components of a given plan are subject to change during the execution of an operation but the intent of the commander for the outcome of an operation and the intent of the commander for each unit involved in conducting the operation are made clear to all concerned during the planning process. Commanders are expected to exercise "good military judgment" during execution of an operation in order to adjust to changes and achieve command intent. General Schwarkopf explained this situation as "Of course military operations are carefully orchestrated, the problem is that some SOB with a grenade jumps in the orchestra pit …"[21]

Step 1a: Partition the Command and Control Problem Space:

The partitioning of the problem space follows from the command intent for a given operation. The current intention of the Army for establishing communication system networks and application system networks to enable composition of components in support of operations is the Common Operating Environment (COE)[22]. The Army COE architecture for achieving the Army Enterprise Network (LandWarNet) is a cloud architecture[23] (see Appendix E). For military operations, a technique often used for summarizing command intent for an operation is a synchronization matrix and an associated graphics overlay summarizing unit activities and locations during different phases of an operation.

---

[19] http://peoc3t.army.mil/c3t/

[20] http://www.brainyquote.com/quotes/quotes/d/dwightdei149111.html

[21] Conversation with the author.

[22] http://ciog6.army.mil/ArmyEnterpriseNetworkVision/tabid/79/Default.aspx

[23] Army Common Operating Environment Architecture, Appendix C to Guidance for 'End State' Army Enterprise Network Architecture, http://ciog6.army.mil/LinkClick.aspx?fileticket=udbujAHXmK0%3D&tabid=79

Step 1b: Assign functional modules to a computational structure:

A wide variety of methods have been used for modeling and simulating joint and coalition operations. The One Semi-Automated Forces (OneSAF) simulation system is the result of decades of experience in matching virtual models to physical unit processes for purposes of training units. A goal of the OneSAF system is to be able to use the simulation system as part of a “mission rehearsal” process for preparing units for execution of operations. One current research effort to improve capabilities for understanding offensive, defensive, and stability operations variables is the DARPA “Deep Green” project.

Step 1c: Establish Communication Between Modules:

Command and Control architectures span a large range of temporal and spatial scales and associated communication capabilities. Appendix D and E provide information on previous and current Army ideas and programs with implementing communications systems to support command and control architectures.

Step 2: Choose a set of quality attributes:

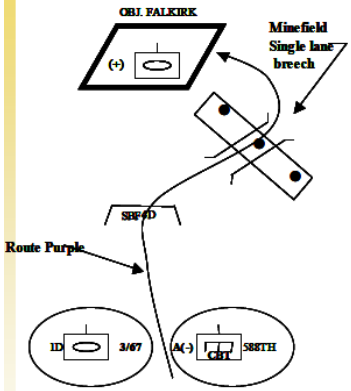
The set of quality attributes are directly associated with meeting the intent of the commander. Often a commander may state specific information requirements in order to support specific decision points associated with a given operation.

Step 3: Choose a set of tasks:

The tasks chosen for the target engagement project described above were (1) time required to reconstitute the defense, (2) effectiveness of the reconstituted defense, (3) relative lethality of the defense (number of air breathing threats and theater missile threats before "leakage"), and (4) relative ability to avoid fratricide.

Step 4: Evaluate the degree with which alternative architectures support the tasks:

For the case of command and control, the need is to support the intent of the commander for offensive operations, defensive operations, and stability operations. This can be as broad as providing humanitarian assistance and disaster recovery (HADR) support to department of homeland security (DHS) efforts during and after a hurricane to providing support to an embedded training team working with Afghanistan National Army (ANA) or Afghanistan National Police (ANP) forces conducting coalition operations against Taliban insurgents.



Phase / Unit	Phase I (move to LOD)	PhaseII (SBF4D)	Phase III (Breech)	Phase IV (Seize obj)
D/3/67 Armor	Occupy positions along LOD	Move to SBF4D	Suppressive fire on objective	Pass through minefield to seize obj
A/3/67 Armor	Occupy positions to feint attack on right flank	Execute feint attack on right flank	Execute feint attack on right flank	Execute feint attack on right flank
B/3/67 Armor	Occupy positions as battalion reserve	Be prepared to assume main attack	Be prepared to assume main attack	Be prepared to assume main attack
A(-)/588th Engineers	Occupy positions behind D/3/67	Move forward behind D/3/67	Execute single-lane minefield breech	Suppressive fire on objective from SBF4D
Artillery	Execute Fire Plan	Suppressive fire on objective	Suppressive fire on objective	On order shift fires behind objective

Figure 5. Synchronization matrix and associated graphics overlay

Step 5: Return to step 1

As indicated above, one approach for commanders to summarize intent for a given operation is to use a synchronization matrix and associated graphics overlay[24]. An example is shown in Figure 5. While Figure 5 depicts mission assignments to battalion subordinate components for an offensive operation, the U. S. Army continues to experiment with a wide variety of approaches to create "trained and ready" units to be prepared to execute offensive, defensive, and stability operations. The US Army Training and Doctrine Command (TRADOC) follows a broad-based approach for creating unit capabilities by considering unit training, doctrine, leader development, materiel, personnel, and facilities variables in achieving and maintaining unit capabilities. The Army readiness reporting system estimates unit combat readiness by considering unit equipment (amount on hand versus amount required and equipment readiness status), unit personnel (soldier availability by number, specialty and experience level), and unit training (status of unit training events). The Army Flow Model is now called the Army Equipping Enterprise System (A2ES)[25] and uses the estimate of force readiness to assist in the Army force generation (ARFORGEN) process of delivering trained and ready brigades with a variety of capabilities.

24 http://www.netscience.usma.edu/workshops/Computational%20Intelligence%20Science%20Approach%20for%20Finding%20Acceptable%20Full%20Spectrum%20Operations%20Not%20Otherwise%20Possible.pdf

25 www.afms1.belvoir.**army**.mil/.../Newsletter%20Jul%2007%20v2.doc

4. Can generalizations be made concerning composed complex system models?

A problem rooted in the issue of resolving differences between continuous time models and discrete time models is the problem of implementing mobile communications networks which enable use of the Internet Protocol (IP). The Internet Protocol is an example of a discrete-event signal but the physical constraints on propagation of electromagnetic waves which "carry" IP signals are represented by the continuous time and space electromagnetic wave equation. Over twenty years ago the commanding general of the Training and Doctrine Command (TRADOC), General Maxwell R. Thurman, visited the MIT Laboratory for Information and Decision Sciences (LIDS). One of the individuals at the LIDS lab, Professor Robert Gallager, was an Army signal officer during the Korean war and had subsequently studied electrical engineering and became an instructor at MIT. During the 1960s and 1970s he and his students had led development of theory and engineering tools which were the basis for the packet-based protocols and communication devices which are the building blocks of the Internet. In the late 1980s the Army was in the process of fielding its first division-level mobile communications equipment which supported packet-based digital communications. The Mobile Subscriber Equipment (MSE) solution enabled use of both analog and digital communications signals and was the first Army system to provide the ability to dynamically redefine switching paths for connecting telephone users (i.e. redefine the "phone book" for point-to-point communications links as the network changed). TRADOC was working with GTE to field the MSE devices to Army units and train Army signal units to maintain communications among elements as the division conducted offensive and defensive maneuvers over varied terrain. At any point in time for a maneuvering division about 1/3 of the MSE equipment was in use, about 1/3 was moving, and about 1/3 was being torn down in preparation for moving. However, there was a persistent problem with training soldiers to recreate the phone book (i.e. reallocate available network ids to individual subscribers in divisional units as the network connectivity changed over time). TRADOC had been receiving numerous complaints from the field concerning the soldiers' inability to quickly update the division phone book as the division conducted offensive and defensive maneuvers and the available circuit nodes changed over time. General Thurman asked Professor Gallager if he was aware of a technical solution to the problem. Professor Gallager replied that he knew of a solution. When General Thurman asked about allocating resources to rapidly create a solution to the problem and asked how long it would take to field a solution, Professor Gallagher replied that it would take at least ten years since we would first have to train the engineers to understand how to design and build the equipment which would implement the solution. In the end, a reasonable improvement to the MSE adaptive phone book problem was achieved without redesigning the equipment but the research, development and engineering community is still developing a solution to dynamically achieving mobile, ad-hoc networks (MANETs) for maintaining information flow among mobile devices more than twenty years after General Thurman posed the basic problem to Professor Gallager. Over the intervening twenty years the world-wide web has been created and critical infrastructures of nations around the world are increasingly more dependent upon proper operation of the Internet.

In the past few decades, the ongoing information systems revolution has enabled many advances. Over the past thirty years there has been six orders of magnitude increase in computing, communications, and data

storage capabilities which, much like General Thurman's dilemma, has led to many unanticipated consequences of increased use of information system devices. While the doubling of capabilities every 18 months will cease at some point, we do expect that over the next 15 years there will be an additional three orders of magnitude increase in capabilities. One expected consequence is that the next generation of Army mobile devices to be fielded between 2013 and 2017 should be able to exploit MANET switching solutions to automatically maintain connections among mobile devices[26]. We currently have no scientific basis for predicting expected behaviors from compositions of components for complex systems support so have no way to discover potential benefits or vulnerabilities (cyber or otherwise) prior to construction and use of the devices.

As touched on in the command and control discussion above, the actual delivery of force structure capabilities ("trained and ready" joint and coalition forces) is the result of much more than simply buying a new device which has increased capabilities. At the beginning of World War II the French had a technically superior tank to the tank fielded to the German forces. The French commanders also had more tanks assigned to their forces than were available to German commanders. However, the doctrine and training of the German army was to mass the tanks into armored units which could maneuver with infantry units while the doctrine and training of the French army was to assign tanks individually to infantry units for use as mobile pillboxes. The point is that the French had superior technology for building tanks and had constructed more tanks with superior operational characteristics. However, the use of tanks by the French Army in terms of warfighting doctrine and training soldiers to use the tanks was inferior to the Germans since the Germans massed their tanks into large groups which overwhelmed the lower concentration of French tanks and then exploited the local destruction of French forces by rapidly moving armored units much faster than conventional infantry could move (the "Blitzkreig" warfare). Similarly, today the US DoD is concerned with "asymmetric warfare" in which opponent use of technology (or some newer approach for using existing technology) may be used to defeat US forces which are not "trained and ready" to counter the new technology, tactics, doctrine, or organization which may confer superior combat effectiveness to an opponent. The actual delivery of "trained and ready" joint and coalition forces is a complex mix of many categories of people with diverse backgrounds, many categories of equipment with diverse behaviors and capabilities, and extensive individual and unit training to complete individual and unit tasks. General Dempsey was recently confirmed as the Chairman of the Joint Chiefs of Staff (CJCS). When he was the Commanding General of TRADOC he championed the idea of developing a "training Brain"[27] to facilitate adaptive learning of currently effective tactics, techniques, and procedures (TTP) and assist commanders in training individuals and units in achieving currently feasible capabilities. We currently have only a limited ability to envision how combinations of cyber force capabilities and conventional force capabilities will revolutionize offensive, defensive, and stability operations.

---

[26] Army Common Operating Environment Architecture, Appendix C to Guidance for 'End State' Army Enterprise Network Architecture, http://ciog6.army.mil/LinkClick.aspx?fileticket=udbujAHXmK0%3D&tabid=79

[27] M. E. Dempsey, **Leader Development**, AUSA Magazine, February 2011, Pages 25-28. Downloaded on 16 December 2011 from: http://www.ausa.org/publications/armymagazine/archive/2011/2/Documents/Dempsey_0211.pdf

4.1 A framework for Cyber-Physical Situation Assessment

Jim Albus of the National Institute of Standards and Technology (NIST) led development of a framework for multi-scale systems over twenty years ago. Since its inception, the Real-time Control System (RCS) architecture has been a widely-used framework for "intelligent" control of networked systems. Jim Albus and a previous Chairman of the IEEE CSS TC on Intelligent Robotics, Prof. Alex Meystel, wrote a book[28] which uses the NIST-RCS architecture as an example of building multi-resolutional intelligent systems. A central notion of the framework, which has been widely used for a variety of systems, is that complex adaptive systems exhibit a capacity to achieve "multi-resolution" interaction with the environment. That is, the framework needs to explicitly accommodate a wide variety of temporal and spatial scales.

A national cyber situational awareness architecture for the Department of Defense needs to interact/support three primary customers: (1) The Chairman of the Joint Chiefs of Staff (GEN Dempsey) and his staff including maintenance of networks which support the generation, selection, and execution of command chain decisions by the national command authority - including conveyance of any specific NCA command intent for all operations for all COCOMs as well as adaptive learning and training on new TTP similar to the "training brain" idea; (2) The Director of Central Intelligence (GEN Petreaus) and his staff including maintenance of networks which enable understanding of international political dynamics and intelligence support of all COCOMs; and (3) the CYBERCOM Commander/NSA Director (GEN Alexander) and his staffs including maintenance of networks which provide information system capabilities to enable NSA support for all COCOMs and CYBERCOM interactions with all other COCOMs and conduct of cyber operations in support of national command authority intent. To provide this broad range of support, a national cyber situational awareness architecture needs to also interact with the network operations centers of other nations as well as those of government agencies, especially the Department of Justice, the Department of State, and the Department of Homeland Security. Thus, a "mission statement" for a national cyber situational awareness architecture should contain a short description of expected capabilities and expected customers. Such a statement would facilitate understanding of the role to be played by a cyber situational awareness architecture in enabling future warfighting roles (both cyber operations by themselves and cyber operations conducted as joint operations with conventional warfighting forces). For the Army components of COCOMs, the categories of operations to be supported are: offensive operations, defensive operations, and stability (e.g. peacekeeping/humanitarian/COIN) operations.

Concerning "cyber terrain", whatever is agreed to as the definition of cyber terrain needs to enable generation of alternative courses of action, analysis of alternative courses of action, and execution of the chosen course of action for a given operation (whether a given operation being considered/supported is at a strategic, operational, or tactical level and whether the operation is an offensive, defensive, or stability operation). The definition and use of cyber terrain should mesh with other elements of warfighting doctrine. For example, the Army has initiated a new Mission Command Center at Fort Leavenworth, http://www.ftleavenworthlamp.com/features/x782434666/Caslen-discusses-mission-command-at-AUSA ,

[28] Alexander M. Meystel and James S. Albus, **Intelligent Systems Architecture, Design, and Control**.

to develop future warfighting doctrine including concepts for integrating conventional capabilities with electronic warfare capabilities and cyber capabilities. LTG Caslen, the commanding general of the Combined Arms Center at Fort Leavenworth has the job that GEN Petreaus had when he led development of the joint Army/Marine COIN doctrine which has been executed the past few years in Iraq and Afghanistan, http://usacac.army.mil/cac2/coin/repository/FM_3-24_English(Dec06).pdf . In order to support the "mission command" set of operations (offensive, defensive and stability), the cyber terrain to be considered is necessarily more complex than an understanding of "network topology and node properties". That is, while there are unique properties associated with cyber warfare (e.g. possible speed of execution, possible ambiguity of attribution of malicious activities, distributed nature of execution, and difficulty of identifying associated outcomes), the command decisions concerning use of a cyber weapon or analysis of the effect of enemy use of a cyber weapon will not be based on a consideration of the network topology or node properties but on the physical outcomes estimated to be caused by the cyber weapon. That is, we should consider cyber-physical estimates of outcomes of cyber weapon use. The cyber terrain of interest is the cyber-terrain of communication networks, information networks, and social-cognitive networks (a composite network) whose properties/activities are affected by a cyber event. Then for a given set of composite networks, the who, what, when where, why and how questions to be answered are those questions associated with facilitating a particular command intent. The Eagle simulation system was built at TRADOC over two decades ago to provide a knowledge-based approach to estimating warfighting outcomes[29] and explicitly capturing command intent as stated in an operations order. The battle command language used by the Eagle system and the high level language subsequently included in later enhancements of the Eagle simulation system is currently being evaluated for use in Chinese battle simulation systems[30]. Even though the Eagle system made a first cut at understanding the semantics of Operations Orders (OPORDs) over 20 years ago, battle simulation systems remain unable to generate estimates of battlespace state other than tradeoffs of combat systems based upon Lanchester predator-prey models. Efforts like Eagle (and now apparently the Chinese effort) to support semantic analysis of content of written operation orders remain in their infancy. However, the battlespace state is much more complex than how many tanks/trucks/ helicopters have been destroyed. The DARPA Deep Green project has been trying with apparently little success to consider aspects of the "three block war" problem of some things being blown up but also a lot of things being rebuilt and a lot of things depending on local culture and social preferences – the insurgency problem

For example, if the intent is to protect a particular critical infrastructure, then the cyber-physical terrain of interest (the commander's critical information requirements for success in defending the critical infrastructure) include at least (1) the status of those communication, information and social networks which enable successful operation of the critical infrastructure, as well as (2) the status of the processes

[29] J W Ogren, **Command and Staff Training and the Practical Use of the HLA**, http://www.mitre.org/work/tech_papers/tech_papers_00/ogren_command/ogren.pdf

[30] Ma Wei-bing and Zhu Yi-fan, **Interoperability of the Simulation-based Training Support Environment with C4ISR system** , downloaded on 16 December 2011 from: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5777852&tag=1

which define successful operation of the critical infrastructure (e.g. for the power grid these processes include the customer demand processes, the power generation processes, the power transmission processes, the lower-level instantaneous control processes, and the higher-level supervisory control processes). The network topology and node properties may be critical to the proper operation of the critical infrastructure or they may have no impact on the proper operation of the infrastructure.

As another example, consider the recent declarations of General Petreaus that we will not be able to "kill our way out of an insurgency" but that the critical need is to "understand the people of Afghanistan." If the declaration of the need to "understand the people of Afghanistan" is taken as a statement of command intent for information operations in Afghanistan, then the cyber-physical terrain of interest is to "understand" (e.g. analyze, predict and influence/change) a complex set of cultural constraints, personal declarations and activities, and collective (family, tribe, hamlet, village, district and provincial) actions and interactions resulting in support for the Taliban or support for the government of the Islamic republic of Afghanistan (GIROA). This is largely a human intelligence effort supported by influencing the network topology and node processes of information networks which enable collecting and analyzing cyber-physical data about human interactions (who, what, when, where, why, and how) and enabling activities to influence/change perceptions and actions which support one political view or another (including perceptions of personal empowerment, economic opportunity and dynamics, family position and influence, tribal position and influence, social status, and security status and dynamics).

At the level of supporting the CJCS, DCI, and CYBERCOM commander, it is certainly the case that higher-level communication network state can be analyzed in terms of the higher-level network protocols such as the Border Gateway Protocol (BGP) and that lower-level communication network state can be analyzed in terms of lower-level network protocols such as the Transmission Control Protocol (TCP). Also, it is very important to understand (analyze, predict, and change) the higher-level and lower-level communication network state. However, the success or failure of operations led by the CJCS, DCI, and CYBERCOM commanders will also be determined by the high-level and low-level network state of ***complex compositions*** of communication system networks, information system networks, and social/cognitive system networks. That is, the collection of Internet nodes and movement of data by itself is becoming increasing more critical to a wide variety of human activities but the actual cyber-physical outcomes of interest are achieved (identified, selected, planned and executed) through the interactions of compositions of networks. This understanding (analyzing, predicting, and influencing) compositions of networks is the area of study of the West Point Network Science Center, http://www.netscience.usma.edu , and the network science collaborative technology alliance, http://www.ns-cta.org . Thus, the definition of information elements critical to the cyber-physical situational awareness architecture should include not only those elements needed to understand communication network state but also those information elements needed to understand compositions of communication networks, information networks, and social/cognitive networks.

4.2 A Tool for Sharing Protected Information with Selected Users and Groups among Network Nodes

While the Real-Time Control System (RCS) architecture maintained by NIST and summarized in section 4.1 can help build reliable models of real-time distributed systems and the architecture analysis methodology used for analyzing the three distributed real-time complex system architectures summarized in section 3 can assist in analyzing and comparing architecture implementations based on using RCS, the actual implementation of large-scale, complex distributed systems is fundamentally dependent upon a solution for rapidly sharing trusted data among the system nodes. That is, unless we can establish the trustworthiness and provenance of the data used in analyzing the current and future states of a complex system, then any architecture implementation approach and any architecture analysis approach will not provide reliable and useful analytical results concerning current and future states of the complex system. This is especially true for cyber-physical situation analysis since we are dealing with virtual approximations of real events and entities so continual refreshing of trusted data is essential to compare predictions of expected outcomes with measurements of actual outcomes.

Appendix F is taken from a paper accepted for publication and presentation at a systems conference[31]. The paper describes a new capability for "owners" of protected data to quickly and securely share real-time data among networked decision-support and real-time control devices with whom the "owners" of the data have explicitly decided to "share" the data. The service is based upon implementation of a recent formal definition and mathematical result [32]derived from the decades-old Bell-LaPadula information security result[33]. The service provides decision makers a means of securely and automatically sharing critical information across security barriers based upon declaration of sharing policies. The declaration and implementation of information sharing policies based upon a need-to- share has been shown to be compatible with information protection policies based upon a need-to- know. Indeed, the implementation of the need-to- share service is based upon extending the mathematical foundations of need-to-know information security systems (the Bell-LaPadula result of 1973).

4.3 Need for Incremental Fielding of Cyber Situational Awareness Capabilities

As stated above, improved Internet-scale anomaly detection tools are required for closing the gap between current processes and tools for ***cyber situational awareness*** and current decision support capabilities for

---

[31] J. James, F. Mabry, and K. Huggins**, Seeing the Real World: Sharing Protected Data In Real Time**, Proceedings of the Hawaii International Conference on System Science (HICSS 2012), January 4-72012, Maui, Hawaii.

[32] James, John R., Frank Mabry, Kevin Huggins, Michael Miller, Thomas Cook, Florian Tamang, Sam Abbott-McCune, Howard Taylor and William J. Adams. Secure Computer Systems: Extensions to the Bell-La Padula Model. http://www.netscience.usma.edu/publications/report1.pdf

[33] Bell, D. E., & LaPadula, L. (1973). Secure Computer Systems: Mathematical Foundations - Volume I. Mitre Technical Report 2547 .

cyber operations. However, improved *anomaly detection and visualization tools alone are* ***insufficient*** for closing the capabilities gap between awareness and decision. Furthermore, the ongoing information systems revolution drives a need to institutionalize an approach for continual improvement of capabilities through incremental fielding of new cyber situational awareness technologies as newer information systems emerge into widespread use. The architecture comparison approach described above is offered as one approach which supports repeated estimation of cyber and physical system state.

4.4 Cyber Doctrine

Cyber situational awareness capability requirements and performance requirements will be more clearly understood as the Services and Combatant Commands continue to develop cyber doctrine and the tactics, techniques, and procedures for applying cyber situational awareness to operational decision-making processes. It is clear from the emerging decisions regarding offensive cyber operations that cyber doctrine is evolving over time and that future cyber operational decisions will be made in accordance with current cyber doctrine as interpreted and refined in the combatant commands and their subordinate commands. In that regard, for land warfare operations the Army has recently announced the establishment of the Mission Command Center of Excellence[34] at Fort Leavenworth. While the mission command center will be developing war fighting doctrine for offensive, defensive, and stability operations in general, it has been specifically tasked to develop doctrine for electronic warfare and information operations (cyber) as they apply to offensive, defensive, and stability operations. The land warfare cyber doctrine that will be developed by the new center will define the cyber doctrine to be used by the Army component of CYBERCOM. Certainly that doctrine will be affected by the declaration by General Petreaus that the primary situational awareness need of the International Security Assistance Force (ISAF) is to understand the people of Afghanistan. To the extent that other Combatant Commands will face stability operation challenges similar to those in Afghanistan, their primary information needs will probably also be to "understand the people" in their own region and the primary cyber situational awareness need of those combatant command decision makers will probably be an awareness of the status and trustworthiness of those networks used to create and maintain an understanding of "the people" in the area of operations.

While there are many ways to gather data to achieve situational awareness of "the people," an approach often used by Combatant Commands is direct engagement in humanitarian assistance/disaster recovery (HADR) operations (e.g. the US government sponsorship of 10 Provincial Reconstruction Teams (PRTs) in Afghanistan). Another approach is direct involvement of forces in local reconstruction efforts in the unit's area of operations (e.g. the local activities of Army and Marine units in Afghanistan). Both the PRT activities and the unit local reconstruction activities are executed by very small groups of service members and civilians working with a few local leaders. Commanders are expected to "think globally and act locally" since the ultimate "global" outcome in Afghanistan will be determined by the accumulated effects of the local outcomes. However, while senior leaders have discussed the importance of the "strategic corporal" to mission success for at least a decade, there is essentially no cyber situational awareness of either PRT local

[34] http://www.ausa.org/publications/armymagazine/archive/2011/2/Documents/Caslen_Flynn_0211.pdf

activities or unit local reconstruction activities in Afghanistan as they influence achieving an understanding of "the people" or assisting in making decisions to achieve desired outcomes in terms of influencing local economic, political, and social outcomes. One reason for this lack of cyber situational awareness at the lowest tactical level is the current focus on creation of tactical command and control nets (for which we have excellent cyber situational awareness) to the exclusion of creating networks which enable commanders and staffs to rapidly collect and analyze data resulting from the lower level unit direct interactions with "the people." Once a tactical unit goes "outside the wire" of a Combat Out Post (COP) connectivity to broadband information flow is cut off. However, the Internet has been recognized as the only network which connects all parties in Afghanistan and, in fact, an initial effort has begun to exploit the network with the establishment of the Ronna web site which promotes direct interaction and awareness, https://ronna-afghan.harmonieweb.org/Pages/default.aspx.

We believe that a productive approach for achieving cyber-physical situation awareness to support cyber-physical decision support systems is to incrementally achieve capabilities from a level of micro-scale networks to a level of global-scale networks (a *bottom-up approach*). That is, since the detection of critical juncture points between different views of composite networks are most likely to be achieved through detailed understanding of specific interdependencies, the place to start looking for interdependencies is through detailed models of networks at short time scales and small spatial scales and then begin to incrementally exploit those interdependencies that "scale up."

5. Conclusion

This report has summarized recent results in information sharing and discussed an approach for extending previous results for information architecture understanding and comparison. The report has also argued that selective sharing of protected information is fundamental to achieving cyber-physical situation understanding.

National efforts in cyber security awareness should include careful and repeated analyses of interdependencies between cyber events, physical outcomes, and cyber approximations of physical outcomes. The evolutionary nature of cyber capabilities is driven by the continuing information systems revolution and necessarily relegates each estimate of the cyber-physical situation as well as the tools, tactics, techniques, and procedures for estimating the cyber-physical situation to a limited interval of temporal-spatial validity. Thus, there is a continuing need for incremental fielding of capabilities for estimating the cyber-physical situation. The approach proposed here for achieving a capability for incremental fielding of tools for estimating the cyber-physical situation is to achieve a science and a framework for objective experimentation and subjective validation of compositions of components comprising an approximation of the behaviors of the domain of interest. One tool which is described in detail is a tool for selectively sharing protected information among nodes in a distributed architecture. Previous results indicated that each domain of interest will need to be individually understood (i.e. predict future domain states) in order to predict future states of complex systems comprised of compositions of component domains.

Appendix A

Appendix A: An architecture for comparison and incremental construction of complex system models[35]

When designing and building closed-loop communication and control systems, communication and control engineers normally consider only a few "dominant modes" of interest (i.e. the minimal set of modes necessary to elicit/coerce the desired behaviors from the set of possible behaviors via control components) and the modes are usually fairly close to one another. Such constraints on the scales of interest necessarily limit the accuracy of the models to those temporal and spatial scales which were considered in the design and implementation of the communications and control systems. In this section several examples are provided which require analysis of a wide range of temporal and spatial scales as well as consideration of compositions of discrete and continuous models. It should be noted that two of the cyberspace examples of interest cited in the trustworthy cyberspace strategic plan[36] (health IT and Smart Grid) both require analysis of a wide range of temporal and spatial scales as well as consideration of compositions of discrete and continuous models.

For the case of power generation and distribution systems, it has been recognized for some time that an interconnected set of power generation and distribution devices constitute a "stiff system[37]" in that the behavior of the interconnected sets of devices is most accurately modeled by a set of dynamic modes which are separated over several orders of magnitude in time and space (e.g. from a time scale of a few tens of milliseconds for wide-area control of the frequency of a 60 Hertz (Hz) electromagnetic wave to a time scale of a few tens of years to consider the effects of sunspot activity on tripping transmission line protective circuits). Likewise, for air defense engagement systems, temporal and spatial scales of interest are driven by the wide range of velocities of potential targets (from zero miles per hour for helicopters to thousands of miles per hour for theater ballistic missiles) and engagement ranges of potential intercept systems. Also, for military command and control systems, temporal and spatial scales range from a few seconds and a few kilometers for control of direct fire engagements by combat crews to several months and perhaps thousands of kilometers for national-level campaigns with coalition partners. Similarly, recent

[35] The architecture comparison approach outlined here is a modification of the one reported in J. James and R. McClain "Tools and Techniques for Evaluating Control Architecture," **Proceedings of the 1999 IEEE International Symposium on Computer Aided Control System Design**, Kohala Coast, HI , USA, August 22-27, 1999, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=808706

[36] Executive Office of the President, **Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program**, page 3.

[37] John J. D'Azzo and Constanstine H. Houpis, "**Linear Control System Analysis and Design**," McGraw-Hill, 1975, pages 38 and 44-45.

events (e.g. the Stuxnet worm[38]) have indicated that critical infrastructures in most if not all countries are now subject to temporal and spatial scales over a range of several orders of magnitude for the "dominant modes of interest" for different cyber-physical effects (e.g. the propagation of the Stuxnet worm may have taken place on a time scale of several months but the time scale involved in destruction of the infected centrifuges via their automated controllers was orders of magnitude faster). The necessity of accommodating a wide range of modes of control opens the possibility of having anomalous operations occur in response to deliberate or inadvertent cyber events as the result of system nonlinearities which introduce behaviors which are harmonics of controlled modes (e.g. multiples of 60Hz as the fundamental mode of power systems generation and distribution systems and multiples of 400 Hz as the fundamental frequency for some avionics control systems).

A modification to an existing architecture analysis approach will first be made in order to establish a framework for comparison of situation assessment analytical results. This will be followed by analysis of situation assessment architectures for: (1) control of air defense engagements which include defense against helicopters, fixed-wing aircraft, and theater ballistic missiles threats, (2) control of electric power generation and distribution systems, and (3) command and control of military forces. With the growing use of the Internet to achieve cost-effective links between management information systems and closed-loop control systems, we conclude the section with an observation that all of the nation's critical infrastructures are now to some extent similarly best modeled as systems whose proper operation is understood through compositions of discrete and continuous models which exhibit a wide range of temporal and spatial scales.

Large-scale, distributed systems (e.g. power distribution systems, factory control, communication networks, distributed simulation networks, military command and control systems) have been growing in size and complexity. Tools and techniques for analysis of these systems have also been changing. One approach for dealing with the growing size and complexity of distributed systems has been to improve techniques for partitioning the problem into sub-problems and arranging these system components into a system architecture. Technologies for building and using reference architectures as a means of lowering costs and increasing reliability of large-scale product-line systems have recently been developed [1, 8, 9] but the technologies are still in their infancy. To be useful in practice, a reference architecture must lend itself to incremental development, testing, and implementation (i.e. the "build a little, test a little" approach of the spiral development model). A necessary capability to achieving the "build a little, test a little" approach to software development is the ability to compare alternative architectures. This appendix uses descriptive terms developed or applied during the Defense Advanced Research Projects Agency (DARPA) Domain-Specific Software Architectures (DSSA) component-based software program [1, 2] to describe constructing and comparing reference architectures. The Department of Defense DSSA program was the first national effort to develop definitions, processes, and tools for component-based software [1,2]. The Department of Commerce subsequently sponsored an Advanced Technology Program (ATP) effort in component-based software [3] to jump-start commercial development of products to enable a component-based software

[38] Stuxnet and Iran's Nuclear Program, James Grayson, March 7, 2011. Downloaded on November 28 20110 from http://large.stanford.edu/courses/2011/ph241/grayson2/

industry. There are now an increasing number of emerging industry standards (e.g. OMG's CORBA and OOAD, Microsoft's COM and DCOM), languages (e.g. C++, Java, and UML) and tools (e.g. Rational Rose) to support component-based software development and maintenance. UML is a widely-used architecture description language (ADL) for building component models and XML is a widely used interface definition language (IDL) for creating messages between components. The current rapid increase in cloud computing is based upon implementations of architecture components which rely on reusable components for implementing capabilities for Software as a Service (SaaS), Provisioning as a Service (PaaS), and Infrastructure as a Service (IaaS) cloud-based information system services.

An Early Architecture Analysis Methodology

The Software Architecture Analysis Method (SAAM) [4] was proposed as a methodology for comparing alternative software architectures. The SAAM architecture analysis steps are:

1. Characterize a canonical functional partitioning for the domain.
2. Map the functional partitioning onto the architecture's structural decomposition.
3. Choose a set of quality attributes with which to assess the architecture.
4. Choose a set of concrete tasks that test the desired quality attributes.
5. Evaluate the degree to which each architecture provides support for each task.

However, while SAAM provides a methodology for architecture comparison, it must be modified for use in evaluating distributed, real-time architectures. Specifically, SAAM is incomplete for comparing alternative distributed, real-time architectures. The incompleteness occurs in two areas: (1) explicit consideration of communication between architectural components is not discussed and is fundamental to distributed, real-time architectures since communications links in an application architecture may vary over time between zero bandwidth and essentially infinite bandwidth, and (2) distributed, real-time processes contain many feedback loops which result in: (a) a need to analyze a set of components to determine the next state of the set of components (i.e. it is not correct to analyze a component in isolation) and (b) the notion of letting a set of components "settle out" over a period of time before the next set of input values are processed (i.e. the idea of a time constant associated with a process).

Concerning the first SAAM incompleteness issue, communication can often be assumed to not be an issue, especially whenever the architecture under consideration will be implemented such that communication between modules is almost instantaneous. Even in this case, communication between modules probably should be accounted for at the reference architecture level. However, for architectures involving large distributed systems, analyzing communications processes between modules is necessary and will normally involve at least a fixed delay (latency) of messages at the simplest level and, for complex systems, may require use of specialized tools to record or simulate actual message preparation, transmission, propagation, receiving, and processing activities. Certainly for our domain of interest, distributed real-time systems, communication is an integral member of the problem space and must be explicitly considered. Establishing communication between modules should be a step in the architecture development process, equal with partitioning the problem space and assigning functional modules to a structure.

Concerning the second SAAM incompleteness issue, the canonical functional partitioning will normally result in components whose internal state depends only on the previous state and current inputs. The component independence assumption is true most of the time for those components supporting higher-level decisions leading to engagement events, especially force operations decisions which set the environment for use of deadly force. However, the component independence assumption is almost never true for modeling lower-level physical processes, such as aircraft and missile guidance control, sensor control, and control of engagement processes, all of which are integral processes of the distributed, real-time problem space. Stated another way, for military applications, the failure of the independence assumption for distributed, real-time components arises from the fact that the distributed nature of motion in the battlespace (e.g. ships, missiles, aircraft, tanks, helicopters, troops, …) means that very high-level decisions can result in producing constraints which dramatically change the operational environment for low-level components. The low-level components then quickly produce different outputs which change the state of the higher-level components inside their decision cycle (i.e. the component independence assumption is invalid because we have a mixed-signal, or hybrid, problem space). Similarly, for critical infrastructure processes complex feedback processes between high-level decisions and low-level system dynamics invalidate an assumption of component independence.

A Distributed, Real-time Architecture Comparison Approach:

While functional segmentation is a natural approach to follow in construction of software modules (since implemented functionality of software process models and data schema can be directly related to user functional requirements), the functional partitioning of components may not be the best approach for architecture development. An architectural comparison approach is thus required. The relative ability of alternative software, hardware and communications architectures to react to expected failure modes will be determined by the detailed partitioning of required operations into functional modules, the mapping of resulting distributed software processes onto the distributed computation and communication resources, and the execution of combined system functionality across components which may be widely distributed in space and time. Recent interest in network science supports consideration of components which comprise a network of communication devices (primarily a hardware layer), components which comprise a network of application components (primarily a software layer), and components which comprise a social network of individuals collectively involved in the domain under review.

An approach for comparing alternative distributed, real-time software architectures:

1. Begin by identifying a (set of) system invariant(s) which determine component equilibrium points around which system rates of change tend to zero and then proceed to build a set of software architectures for the distributed, real-time problem space by repeatedly:
    - a.1 Identifying the level above which system behavior is to be determined by modifying logical parameters only and partition the problem space (tasks) into appropriate higher-level functional modules using event-based models (i.e. capture the enterprise logical dynamics and compare the logical model behaviors with observed logical behaviors),

a.2. Below the level identified in step a.1, partitioning the problem space (tasks) into functional modules, some strictly event-based models, some a mixture of event-based models and differential-algebraic-equation-based models (i.e. capture the enterprise physical dynamics and compare the physical model behaviors with observed physical behaviors).

b. Assigning modules to a computational structure (usually pipe and filter computational style), and

c. Establishing communication between modules.

2. Choosing a set of quality attributes with which to assess the architectures (pick success criteria),
3. Choosing a set of concrete tasks which test the desired quality attributes, and
4. Evaluating the degree to which each architecture provides support for each task.
5. Returning to step 1.

References

[1] Boehm, B. W. and Scherlis, W. L. "Megaprogramming," Proceedings of the DARPA Soft ware Technology Conference, April 1992

[2] Mettala, E. G., James, J. R., Coleman, N., Gallagher, E. J., Harris, R. L., Smith, J. G., and Graham, M. "Domain-Specific Software Architectures: Government Needs and Expectations." Proceedings of the IEEE Symposium on Computer-Aided Control System Design, Napa, CA 17-19 March, 1992.

[3] Benefits and Costs of ATP Investments in Component-Based Software, 1997 http://www.atp.nist.gov/eao/gcr02-834/references.htm

Appendix B

Appendix B: A network challenge for situation assessment of air defense engagements

The complex system modeling example discussed in this appendix was performed at Lockheed Advanced Technology Laboratories over a decade ago the material provided here is based upon a paper presented at a technical conference[39]. Air defense command and control usually places airborne entities into one of three categories, friendly, enemy, or unknown. In the past, air defense engagements have resulted in a number of events in which friendly aircraft or civilian aircraft were mistaken for hostile targets and destroyed. A continuing effort of situation assessment for air defense engagements is to comply with the laws of land warfare for engaging aircraft with hostile fires. While self defense is always a reason for engaging hostile aircraft, engaging potential targets after receiving fire would be an attempt to extract revenge while engaging hostile threats before they destroy their intended targets would be an attempt to protect valuable assets. Thus, a key element of air defense engagements is to assess the situation in terms of the relative level of hostilities among potential combatants and the norms of airspace use in order to determine if a potential target should be engaged prior to the target releasing a weapon. This section will not cover the various means for developing the Rules of Engagement (RoE) but simply observe that as the RoE become less restrictive the probabilities of mistakenly engaging friendly aircraft or non-combatant aircraft increase and also note that one of the constraints on network information systems is to both (1) rapidly and reliably identify non-combatant, friendly, and hostile targets and also (2) rapidly share changes to the RoE as the situation develops.

While command and control of military operations is a group decision-making process (i.e. social network process) which can take many months for national-level coalition operations, there is a rapid reaction group decision making process for target engagement which is often known as a combat crew drill. This section provides an overview of information system support for combat crew drills associated with engaging potential airborne targets.

A consistent issue in conceiving, designing, and constructing computer-controlled systems is achieving adequate models of system components and determining which components are independent of other components or the nature of interdependencies between components. The arrangement of relationships between dependent and independent components is then used to determine the system architecture. Modification of the behavior of the network of components comprising the system architecture is the central task of control engineering. Classical design approaches focus on single-variable and multivariable

[39] The air defense engagement process partitioning problem presented here is a modification of the one reported in J. James and R. McClain "Tools and Techniques for Evaluating Control Architecture," **Proceedings of the 1999 IEEE International Symposium on Computer Aided Control System Design**, Kohala Coast, HI , USA, August 22-27, 1999, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=808706

components whose dynamical models are independent of each other. However, interest in discrete-event dynamical systems and the growth of hybrid systems tools and techniques has created the need to evaluate event-based components as well as components whose models include both discrete logic and continuously evolving variables. The mixed-signal issues of hybrid systems analytical problems have been encountered repeatedly in the field of artificial intelligence as the "pixel-to-predicate" problem for vision understanding or the "sensor-to-shooter" problem for military applications. An Internal Research and Development effort at Lockheed Advanced Technology Laboratories was undertaken over a decade ago to develop an approach for evaluation of alternative architectures for control of large-scale, networked systems whose components may or may not be independent and whose activities are distributed in time and space. This appendix provides an overview of the approach developed and discuss how it can be applied to evaluate alternative architectures for control of large-scale, distributed systems and for analysis of approaches for recovery from various system failure modes. There is a fundamental man-in-the-loop decision cycle for ballistic missile air defense engagements associated with events which occur from the time of a Ballistic Missile threat launch through the time of intercept and assessment of engagement outcomes to determine whether the target must be re-engaged (Figure 1).

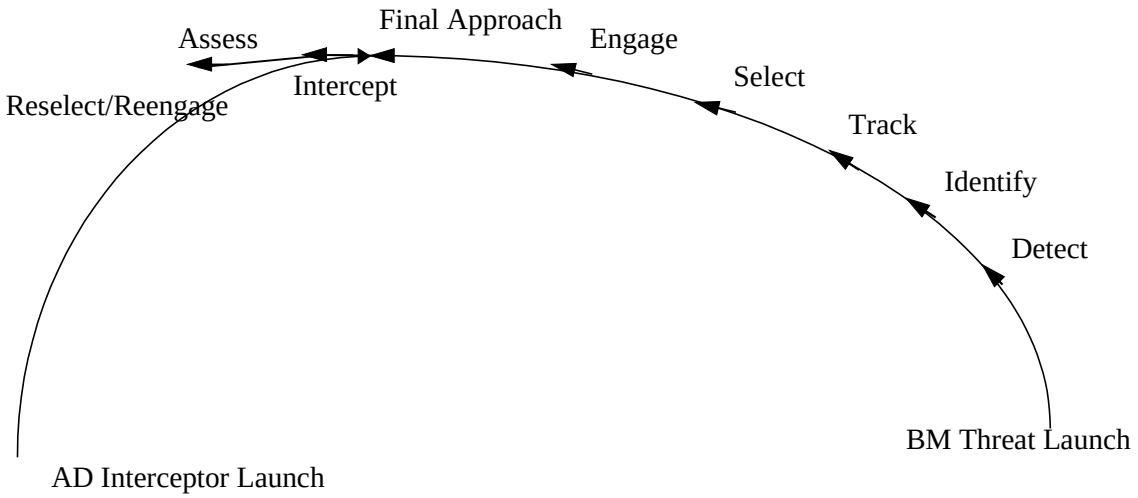


Figure 1. Ballistic Missile Engagement Sequence

Discussion of the Air Defense Engagement Problem

Large-scale, distributed systems (e.g. power distribution systems, factory control, communication networks, distributed simulation networks, military command and control systems) have been growing in size and complexity. Tools and techniques for analysis of these systems have also been changing. One approach for dealing with the growing size and complexity of distributed systems has been to improve techniques for partitioning the problem into sub-problems and arranging these system components into a system architecture. Technologies for building and using reference architectures as a means of lowering costs and increasing reliability of large-scale product-line systems have recently been developed [1, 8, 9] but the technologies are still in their infancy. To be useful in practice, a reference architecture must lend itself to

incremental development, testing, and implementation (i.e. the "build a little, test a little" approach of the spiral development model). A necessary capability to achieving the "build a little, test a little" approach to software development is the ability to compare alternative architectures. Thus, this appendix applies an architecture comparison approach described in Appendix A as part of the reference architecture development process. This appendix uses descriptive terms developed or applied during the Defense Advanced Research Projects Agency (DARPA) Domain-Specific Software Architectures (DSSA) component-based software program [1, 2] to describe constructing and comparing reference architectures. The Department of Defense DSSA program was the first national effort to develop definitions, processes, and tools for component-based software [1,2].

Comparing Architectures for Air Defense Engagement

A comparison of Engagement Operations architectures for air defense operations was conducted during an Internal Research and Development (IRAD) project [10]. That project evaluated alternative approaches for providing air defense of maneuver forces for missile (ballistic and cruise missiles) and air-breathing (fixed-wing and rotary-wing) threats. The project involved modifying the Extended Air Defense Simulation (EADSIM) program to support architecture analysis. EADSIM is a high-fidelity (about 500,000 lines of c and Fortran code) program which models the logic and dynamics of air-defense engagement processes. The statement that the architecture analysis approach begins with identifying system fixed points (system invariants) is a new assertion. This was an assumed condition for the air defense engagement process since persistent models of system dynamics are in fact constructed around system fixed points.

Step 1a: Partition the Engagement Operations Problem Space:

While the Corps air defense problem is a very large one, resource constraints led us to restrict ourselves to a subset of the problem space. Specifically, we were not able to examine in detail the continuous systems modeling components of the Extended Air Defense Simulation (EADSIM) (flight, sensor and propagation processes) but have studied the Flexible Commander logic implementation within the command and control logical process. The EADSIM solution is a strictly hierarchical one (as opposed to a more flexible netted, distributed one) where each commander deconflicts feasible engagements for subordinates and assigns targets to each assigned weapon system.

In this context, our consideration of the Architecture Analysis Methodology (AAM) problem space is restricted to the engagement sequence of Engagement Operations summarized in figure 1. Interrupting the EADSIM logical simulation process supports simulating alternative architectural approaches to implementing software support to engagement operations. Modules for detection, identification, tracking, selection (allocation), engagement, final approach, engagement assessment, and disengagement or reengagement or new target processes could be implemented. Modules for detection and identification would naturally be concentrated in the unit sensor systems but synchronization with other systems (especially coalition partner and national technical means) require portions of the functionality to be distributed. The sensor fusion problem becomes more complicated as we increase the number of sensor (radar) inputs being integrated locally. Similarly, the tracking problem also becomes harder as track results from local fusion processes must be resolved with more tracks from remote sensor systems. We have

implemented a modification to EADSIM which extends engagement logic (the Flexible Commander module) code to support a netted, distributed (cooperative) approach to target deconfliction (see Figure 1). The system architecture must meet system requirements for successful completion of the engagement sequence of Figure 1 under both nominal conditions and stressed conditions (failure modes). Figure 1 reflects the mixed-signal nature of the problem in depicting the engagement events (which are states in the set of engagement states for each target engaged by each unit) and paths of threat and interceptor missiles (which are represented as sequences of points in four-dimensional space of range, azimuth, elevation and time with respect to each sensor which tracks the motion of each missile). An implementation would be comprised of a hardware architecture, a communication architecture and a software architecture. For purposes of the software architecture comparison we assumed that the hardware and communications architectures were given and proceeded to develop a framework for comparing alternative software architectures.

Step 1b: Assign functional modules to computational structure:

While recognizing that the optimal solution of the target engagement problem is a mixed-signal problem, we restricted our investigation of alternative architecture solutions to implementation of logical components using EADSIM and relied on the unmodified evolution models of EADSIM to model the flight, sensor and propagation processes and provide the values of the evolution variables at the update intervals of the decision logic.

Step 1c: Establish Communication Between Modules:

Alternative software architecture styles [5,6] include: Main/Subroutine, layered (distributed), data abstraction (object-oriented), pipe & filter, repository (blackboard), and event-based (implicit invocation of procedures). The software architecture will probably be required to work with many different hardware architecture configurations, including different numbers of major components. It is expected that alternative hardware choices, such as increases in numbers of sensors or in the number of command and control nodes or alternative functional allocation between sensors, command and control nodes and missiles would require alternative communication capability between system components but these alternatives were not modeled in this effort.

We depended upon EADSIM to simulate communication between other modules. While we expect that different architectural styles will cause different impacts on the communications, without additional modeling of communication details, tradeoffs between architectural styles cannot be analyzed.

Step 2: Choose a set of quality attributes:

The attributes chosen for this project were (1) relative ability to reconstitute the defense and (2) relative ability to engage air defense threats.

Step 3: Choose a set of tasks:

The tasks chosen for this project were (1) time required to reconstitute the defense (effectiveness of the reconstituted defense (3) relative lethality of the defense (number of air breathing threats and theater missile threats before "leakage"), and (4) relative ability to avoid fratricide.

Step 4: Evaluate the degree with which alternative architectures support the tasks:

The modifications to EADSIM were implemented to support comparing a netted, distributed command and control architecture to four other command and control architectures: 2-tier centralized, 1-tier centralized, autonomous tactical operations centers and autonomous surface to air missile batteries. A series of performance cases were run against a total of five architectures to determine the effectiveness and efficiency of each under a range of stressing cases. The five architectures compared were: centralized command with two tiers of command, single tier centralized command, autonomous Tactical Operations Centers (TOCs), autonomous Surface-to-Air Missiles (SAMs), and the new coordinated structure using a nearest neighbor coordination algorithm. The netted architecture was setup to coordinate TOCS at the same command tier (peer-to-peer). We measured both effectiveness (the percentage of targets killed) and efficiency (number of kills per missile) of each architecture to provide a more complete measure of the overall systems utility than simply measuring kills.

Step 5: Return to step 1

Common Details in the Testing Scenario

Five alternative C3I architectures were implemented and compared by evaluating the performance of each one against an identical series of missile attacks of increasing intensity. Each architecture defends 3 point assets. Each architecture has equivalent defensive fire power at its disposal: 4 surface-to-air missile (SAM) units consisting of a radar and launcher combination. The fire unit behaviors were implemented with a Flexible SAM ruleset. The Autonomous SAM command and control architecture is shown in Figure 2.

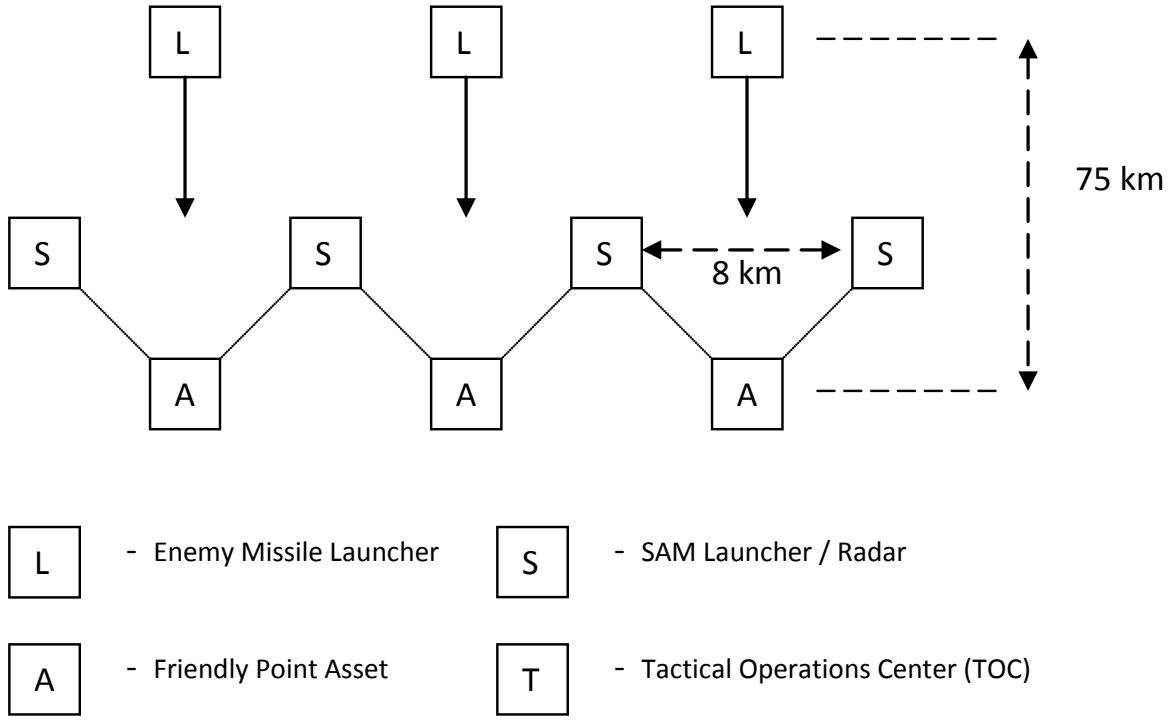


Figure 2. Autonomous SAMs

Hostile Missile Attacks – The 3 hostile missile launchers generate a wave of depressed trajectory missiles at the 3 friendly assets during a 6 minute scenario. Six enemy laydown files with increasing rate of missile launchings were prepared and used against each architecture. The probability of kill of the enemy missile

was set to 100% to simplify the outcome bookeeping. (Each enemy kill or rekill counts as one leaker, and, equivalently, each enemy miss counts as an intercepted missile for the defense).

SAM Fire Unit – The 4 defensive fire units were provided with an essentially unlimited supply of missiles so that the limitation to the defense would lie in the C2 ruleset for the SAM unit. The SAM ruleset firing doctrine was set to take up to 2 shots at each target (Shoot-Shoot). The SAM was limited to having 2 missiles in the air at a time. The distribute fire flag was selected, so that the ruleset would distribute its 2 shots against 2 targets in the event that it had more than one threat in its trackfile. The probability of kill of the interceptor was set to 85%.

Communications – For the achitectures where TOCs control SAMs, communications between the TOC and SAM take place over a dedicated 76800 baud link. A three-dimensional view of the EADSIM output is shown in Figure 3.

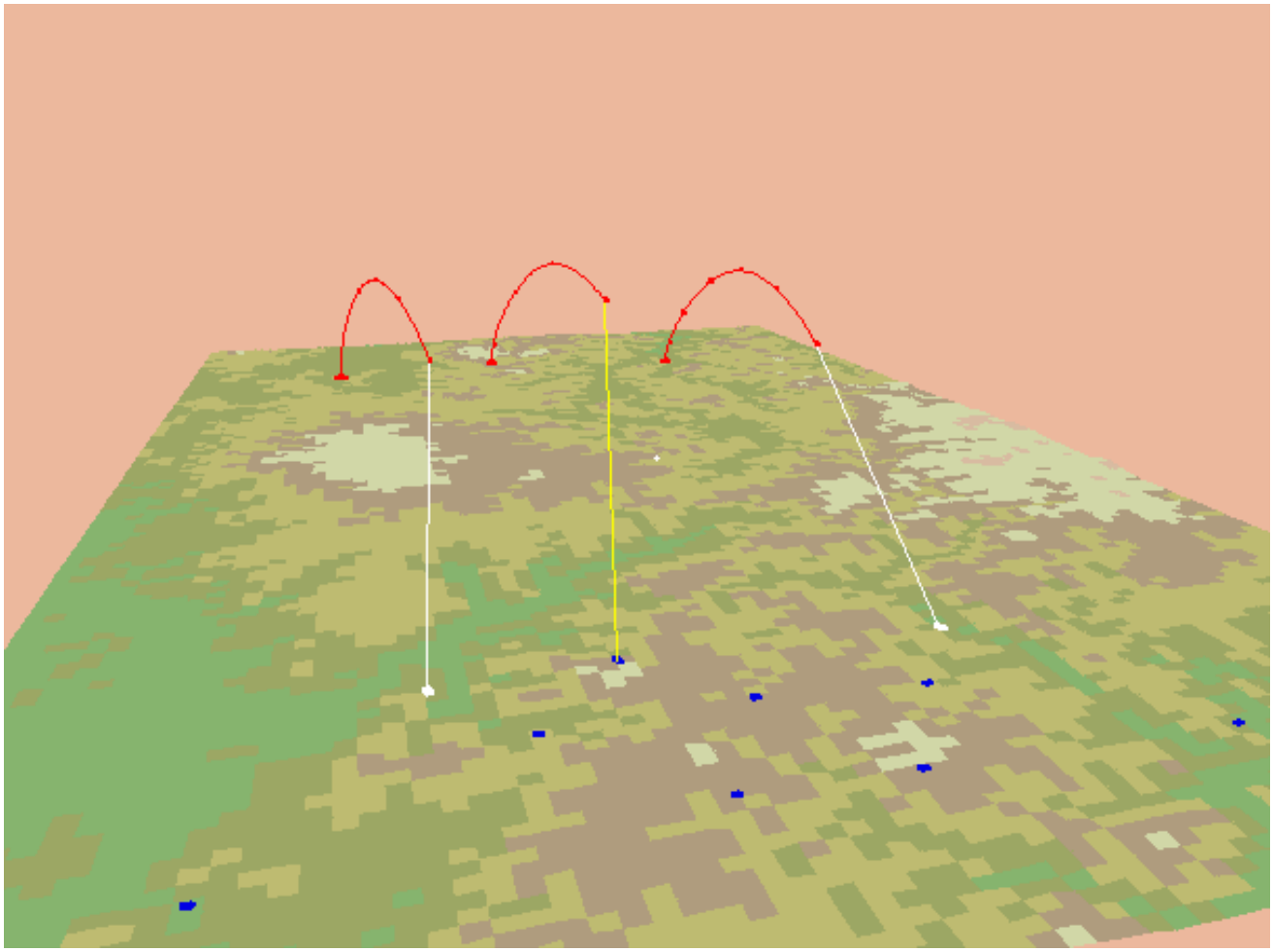


Figure 3. EADSIM 3-Dimensional Output

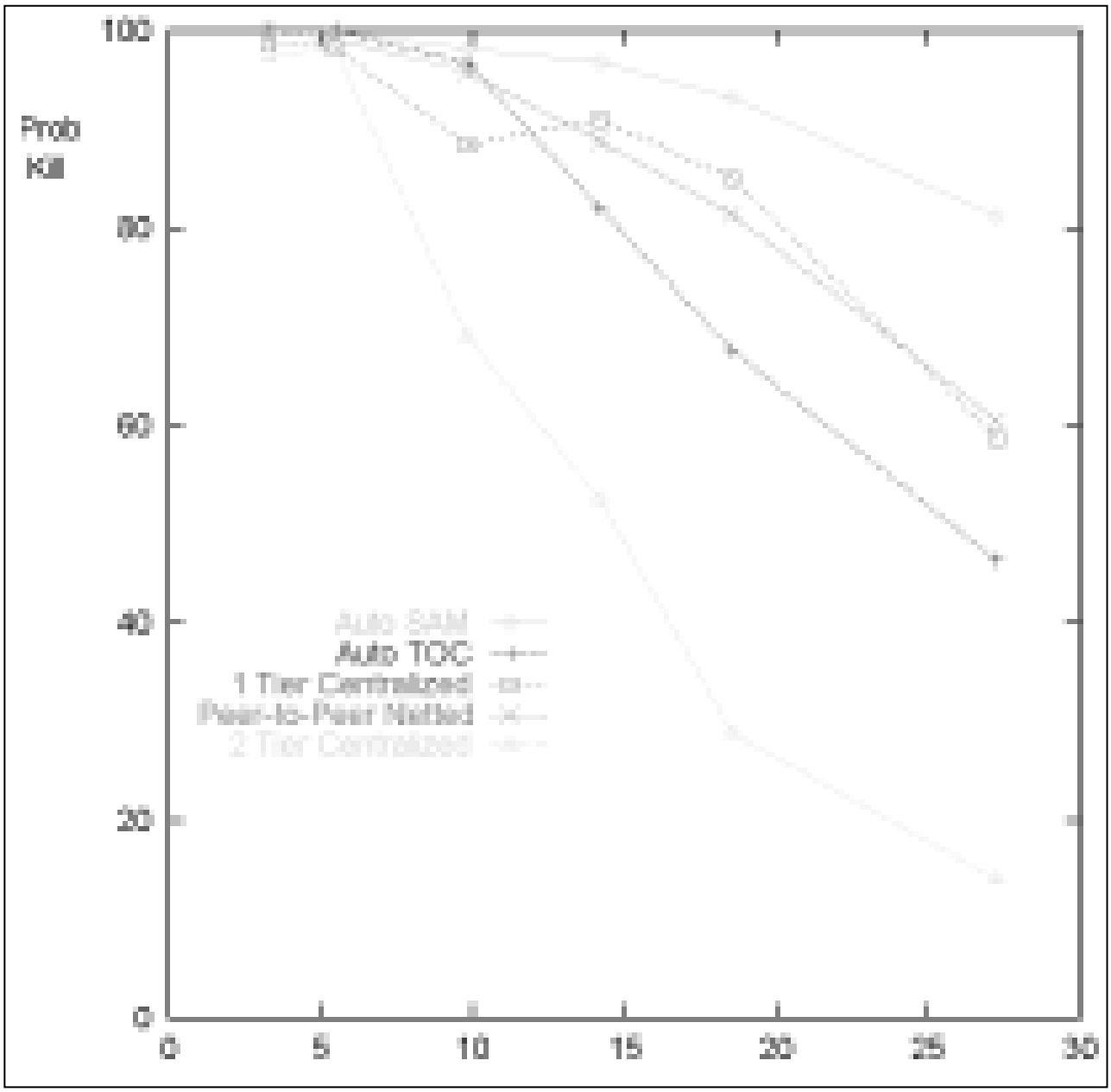


Figure 4. Probability of destroying incoming missiles versus intensity of a missile attack.

The architectures divide into roughly three categories of behavior. The most effective defense against all intensities is seen to be the Autonomous SAMs. The three architectures that have a single tier command structure show some differences, but tend to cluster together at the midrange of effectiveness over all intensities. The least effective defense against all intensities except the least intense is seen to be the Two Tier Centralized.

Conclusion

We have described initial efforts to establish tools and techniques for evaluating alternative control architectures for large-scale, distributed systems. More work is needed for tools and techniques to support development and deployment of such systems.

References

[1] Boehm, B. W. and Scherlis, W. L. "Megaprogramming," Proceedings of the DARPA Soft ware Technology Conference, April 1992

[2] Mettala, E. G., James, J. R., Coleman, N., Gallagher, E. J., Harris, R. L., Smith, J. G., and Graham, M. "Domain-Specific Software Architectures: Government Needs and Expectations." Proceedings of the IEEE Symposium on Computer-Aided Control System Design, Napa, CA 17-19 March, 1992.

[3] Benefits and Costs of ATP Investments in Component-Based Software, 1997 http://www.atp.nist.gov/eao/gcr02-834/references.htm

[4] Kazman, R, L. Bassm G. Aboud, and M. Webb "SAAM: A Method for Analyzing the Properties of Software Architectures", http://www.sei.cmu.edu/library/abstracts/whitepapers/icse16.cfm , 1995.

[5] Garlan, D, and M. Shaw "An Introduction to Software Architecture", January, 1994. http://www.cs.cmu.edu/afs/cs/project/able/ftp/intro_softarch/intro_softarch.pdf

[6] Abd-Allah, A, and B. Boehm, "Models for Composing Heterogeneous Software Architectures" USC Technical Report 96-505, http://csse.usc.edu/csse/TECHRPTS/1996/usccse96-505/usccse96-505.pdf

[7] Tracz, W., and Coglianese, L. "An Adaptable Software Architecture for Integrated Avionics" ADAGE-IBM-93-03. IBM Federal Systems Division.

[8] Hayes-Roth, F., Erman, L. D., Terry, A., and Hayes-Roth, B., "Distributed Intelligent Control and Management (DICAM) Applications and Support for Semi-Automated Development." Proceedings of AAAI-92 Workshop on Automating Software Development, San Jose, CA, 1992.

[9] Vestal, S. " Integrating Control and Software Views in a CACE/CASE Toolset," Proceedings of the Joint IEEE/IFAC Symposium on Computer-Aided Control System Design, Tucson, AZ, 6-9 March, 1994.

Appendix C

Appendix C: A network challenge for situation assessment of the smart grid

This appendix describes an approach for modeling smart grid dynamics as a set of interdependent composite networks. The majority of the section has been taken from a paper prepared with Dr. Aaron St Leger as part of a project sponsored by the Defense Threat Reduction Agency (DTRA) and co-authored by Dr. Dean Frederick.[40] A composite network is one whose evolution in time and/or space is described as a composition of more than one category of networks. This work utilizes an interconnection of communication network, information network, and a power system network to model smart grids. More specifically the modeling focuses on bulk generation and transmission of power. The resulting model is proposed for studying and simulating wide area measurement and control techniques and contingencies. The modeling methodology is based on the initial partitioning by the National Institute of Standards and Technology (NIST) of the smart grid domains. Some initial results of modeling a small portion of a future smart grid as the composition of a five-bus power generation and distribution network together with an associated communications network capable of setting parameter values (distributing power system set points across communication network nodes) associated with power generation and distribution components is presented.

Introduction

The power grid consists of physical components, which generate and transmit power, and cyber components which transmit data and control signals. Currently, operation and control of bulk power generation and transmission network occurs at centralized control centers and relies mostly on operator in the loop control/analysis. For example, results from state estimation and contingency analysis will be reviewed by operators and adjustments system operation made accordingly by the system operator. This control loop relies on human intervention and the time scale is on the order of minutes. In addition, some automatic wide area control, such as automatic generation control (AGC), have been implemented and relies on a slow response. More specifically "AGC acts slowly and deliberately over tens of seconds or a few minutes" [1]. Current analytical techniques and models make assumptions that communication lines are in service and any latency or bandwidth constraints are negligible and/or have no effect on system operation. With the slow response of current wide area control techniques these assumptions are adequate. However, the advancement and implementation of smart grid technology will require more advanced models that factor in the status and performance of communication networks. For example, results presented in [2] show that an increase in time delay can cause degradation of frequency control using decentralized intelligent loads and lead to system instability. As a result, the present state and time-delay of communications can be a critical contingency for smart grid applications. The objective of this work is to

[40] A. St. Leger, J. James, and D. Frederick, Modeling Smart Grids as a Set of Composite Networks, submitted to

develop a modeling methodology for analyzing smart grids, control techniques, and identifying important contingencies within cyber and physical elements of the system. These contingencies could be malicious, for example a cyber or physical attack, or not. A critical component is modeling the interdependencies between the cyber and physical components.

Vulnerability analysis of power systems and information networks is a continuing field of research [3-5]. The focus of many research efforts have been placed on large cascading failures due to impacts of such disruptions. Historically, much research has focused on either the power grid or information networks [6, 7]. Recently the interdependencies of the two infrastructures been studied [3, 8, 9]. The current state-of-the-art techniques rely on qualitative analysis of the systems and interdependencies [5] and, as a result, develop approximate results and estimations of the real interdependencies of the two systems. Some work is moving towards a quantitative approach more suitable for analyzing smart grid applications [10]. The approach described in this paper is to develop a novel unified quantitative methodology of modeling both the cyber and physical components of the system, and the interdependencies between the two. More specifically the focus is on a unified cyber/physical system model suitable for stability analysis of the following:

- Physical contingencies in HV transmission network/bulk power generation
- Cyber contingencies in smart grid components related to HV transmission/bulk Generation
- Decentralized local and wide area control
- Centralized wide area control

Developing a suitable model for smart grid simulation is challenging as the smart grid is still emerging and evolving as technology and control techniques continue to evolve. The modeling methodology presented here is developed in a flexible fashion to allow for implementation of new technology and control schemes. The smart grid as defined by NIST [11], shown in Fig. 1, was used as a starting point for modeling.

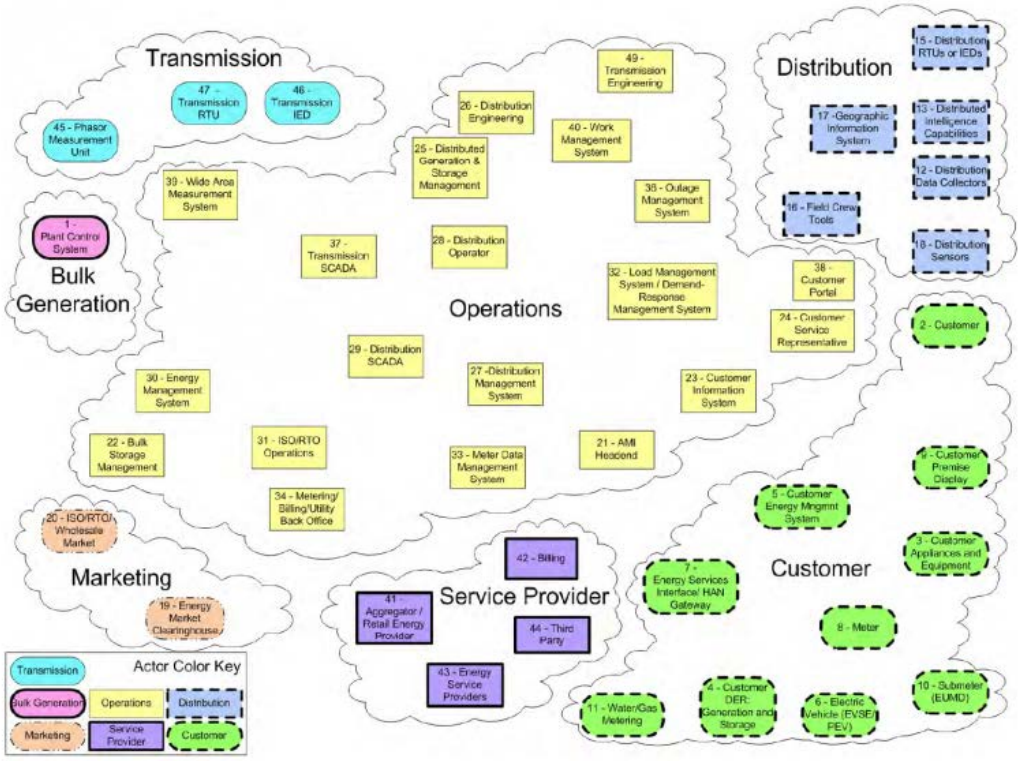


Fig. 1 Actors in the Seven Domains of the Smart Grid

In the next section we will provide an overview of our methodology for modeling the smart grid, including specific details on modeling the power system, communication, and information network components. This is followed by a section showing some initial modeling and simulation of a small system followed by a conclusion.

Smart Grid Modeling Methodology

Only a subset of Smart Grid components, as defined by the seven domains in Fig. 1, is pertinent to HV bulk power transmission network. As a result, only components applicable to the previously outlined analysis are modeled in this work. More specifically, this model includes controls, communications, and power system/communication network dynamics. This aligns with the Bulk Generation, Transmission, and Operations actors. Influence at the HV transmission level from customer loads and the distribution network are modeled aggregately at HV substations. Physical and cyber components within and between these actors are modeled. Initial work has focused on the following:

- Physical components:
  - Generators, loads, transmission network
  - Communication devices (e.g. modems)
  - Communication links (e.g. fiber optic cable)
  - Sensors (e.g. phasor measurement units)
  - Controllers (e.g. voltage regulators, governors).

- Cyber components:
  - Smart grid control logic (e.g. wide area control logic/decision making).
  - Transfer of information between components

The physical and cyber components are modeled separately and linked together in such a way to model the interactions between these components. A general framework of the overall model is shown in Fig. 2. The model incorporates the power system model, consisting of generators, transmission lines, transformers and loads, the communication network model, consisting of communication links between and within components, and local/wide area control. The Local Communication Network and Control (LCNC) models control actions distributed throughout the grid that are taken at a local level. These control actions could depend on local measurement, wide area measurements or both. For example, a smart substation can be modeled as a LCNC model. This model would include algorithms governing smart substation behavior, local measurement/control techniques, and interface with external components via a communication link/network. Remote System Operation and Control (RSOC) is represented in a similar fashion and allows for modeling of wide area control and operation. This model structure passes control commands to the system via the communication network.

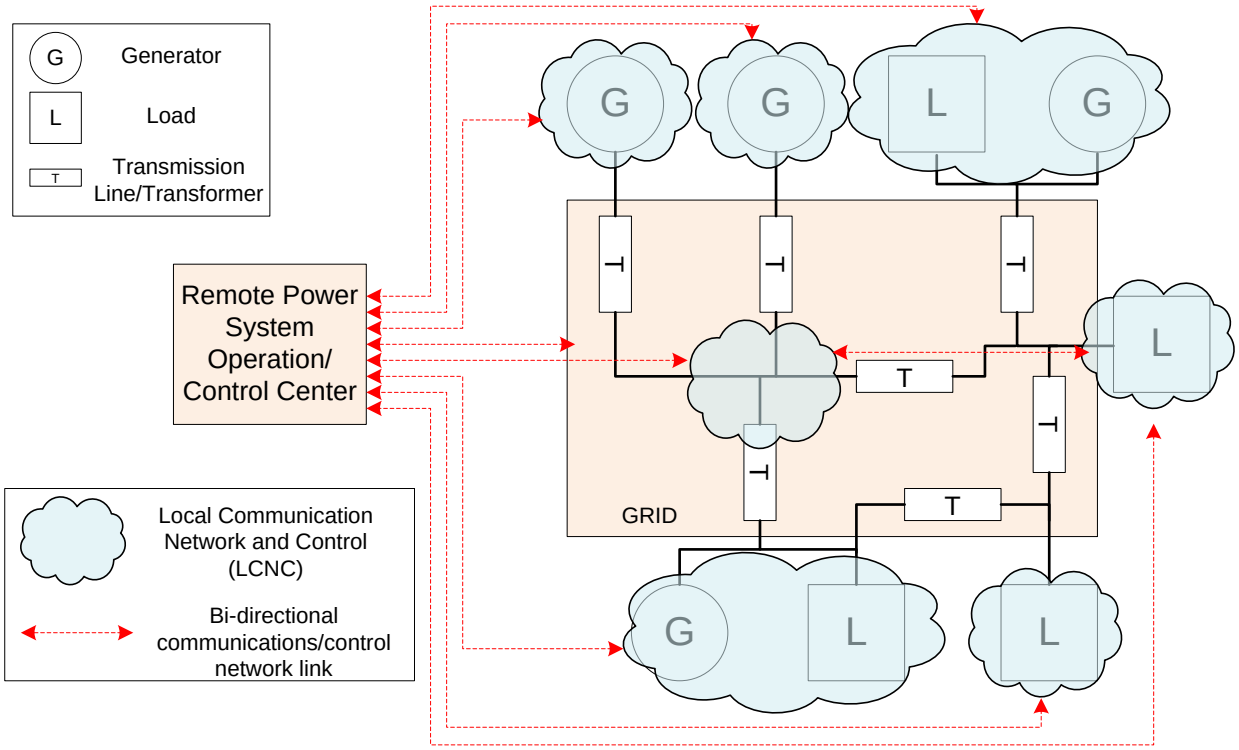


Fig. 2. Smart Grid Model Structure

This general framework of LCNC and RSOC linked to physical model of the power system/communication network is generalized to allow for modeling of a wide range of smart grid devices and controls. The next sections discuss the power system, communication network, and control components in more detail.

A. Power System Network Components

The power system network, which consists of an interconnection of transmission lines and transformers, is modeled by an interconnection of impedances modeling each component. Network equations in terms of the nodal admittance can be written for an n bus system from this as follows [12]:

$$\begin{bmatrix} I_1 \\ I_2 \\ \dots \\ I_n \end{bmatrix} = \begin{bmatrix} Y_{11} & Y_{12} & \dots & Y_{1n} \\ Y_{21} & Y_{22} & \dots & Y_{2n} \\ \dots & \dots & \dots & \dots \\ Y_{n1} & \dots & \dots & Y_{nn} \end{bmatrix} \begin{bmatrix} V_1 \\ V_2 \\ \dots \\ V_n \end{bmatrix} \qquad (1)$$

or

$$\mathbf{I} = Y_{bus}\mathbf{V} \qquad (2)$$

where is the bus admittance matrix, I is a column vector of current injection at the network nodes and V is a column vector of nodal voltages. Generators and loads are modeled as power injections into the system nodes.

Generators are modeled as synchronous machines with a governor, exciter and power system stabilizer. The mechanical model of the generator is based on the swing equation. Details on these models can be seen in [12]. Loads are modeled as constant power. Enhancement of this work is ongoing to incorporate ZIP and dynamic load models based on induction machines.

B. Communication Network Components

Communication network modeling has consisted of two approaches. The first is to model physical devices and communication links (e.g. modems, fiber optic networks, etc). Initial work has incorporated a frequency shift key (FSK) modem to transmit control signals between components. The second approach is a generic communication link model incorporating bandwidth and latency which are the two most inherent properties for smart grid communication as discussed in [13]. The initial model incorporates a variable time-delay to the data sent over a communication link. Work is ongoing to develop time-delay based models to represent specific communication hardware and protocols. However, the initial time-delay model can be used to study the effects of latency on wide area control techniques and other smart grid functions.

C. Control Components

Modeling of control components is broken down into LCNC and RSOC models. RSOC models are used for wide are controllers such as Static Var Compensation (SVC) control in[14]. A model for a SVC in our approach is shown in Fig. 3. Communication links transmit measurements from a phasor measurement unit (PMU) unit embedded in the power system model and deliver it to an algorithm which processes the data,

updates the discrete state of the SVC and send a control signal over a communication link. Different control algorithms, communication links, SVC models, etc. can be modeled.

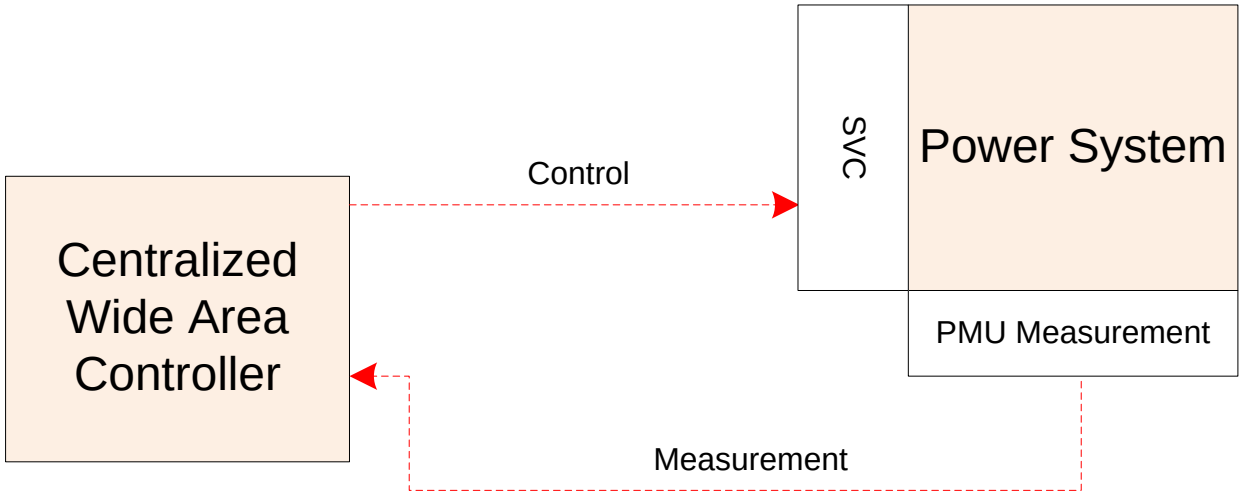


Fig. 3. RSOC Model of Wide Area Control SVC

LCNC models are used for localized control which can be based on local or wide area measurements. For example, power system stabilizer controls are implemented via local measurement and feedback at the generators. Smart grid components requiring wide area measurement or transfer of information between components embedded in the network are modeled as intelligent agents. An intelligent agent is an autonomous, goal-oriented entity that can interact with its environment [13]. This is modeled here as an algorithm dictating the behavior of the agent with local and wide area measurement as inputs while local control actions and communication with other agents as outputs. Latency of local control actions and measurements for LCNC is assumed to be zero. Latency and transmission of information to and from LCNC is represented by the communication network model. The following section discusses initial efforts toward constructing and simulating the proposed smart grid model.

Smart Grid Model Simulation

MATLAB/Simulink [15] has been utilized for constructing and simulating the proposed smart grid model in this work. This software environment is flexible enough to add custom models, adjust pre-existing models, and develop a custom graphical user interface. In addition, co-simulation of discrete and continuous systems is possible. All proposed components have not yet been implemented; however, some initial progress has been made and is presented here. Power system simulation is handled via the SimPowerSystems toolbox. Controllers (generator voltage regulation, power system stabilization, etc.) are implemented via Simulink. Communication components are simulated by a combination of communication toolbox and custom functions. More advanced smart grid controllers and agents are being developed through custom functions interfacing with power system and communication components.

Presently, the IEEE 14 bus system has been implemented with remote control of generator setpoints, power output and voltage magnitude, via a communication link and a FSK modem. In addition,

load control and status of power system components are controllable via FSK modem. This initial work shows a proof of concept of integrating communication, control and power system components which comprise the proposed smart grid model. A specific example of a single machine infinite bus system is shown in Figures 4 and 5.

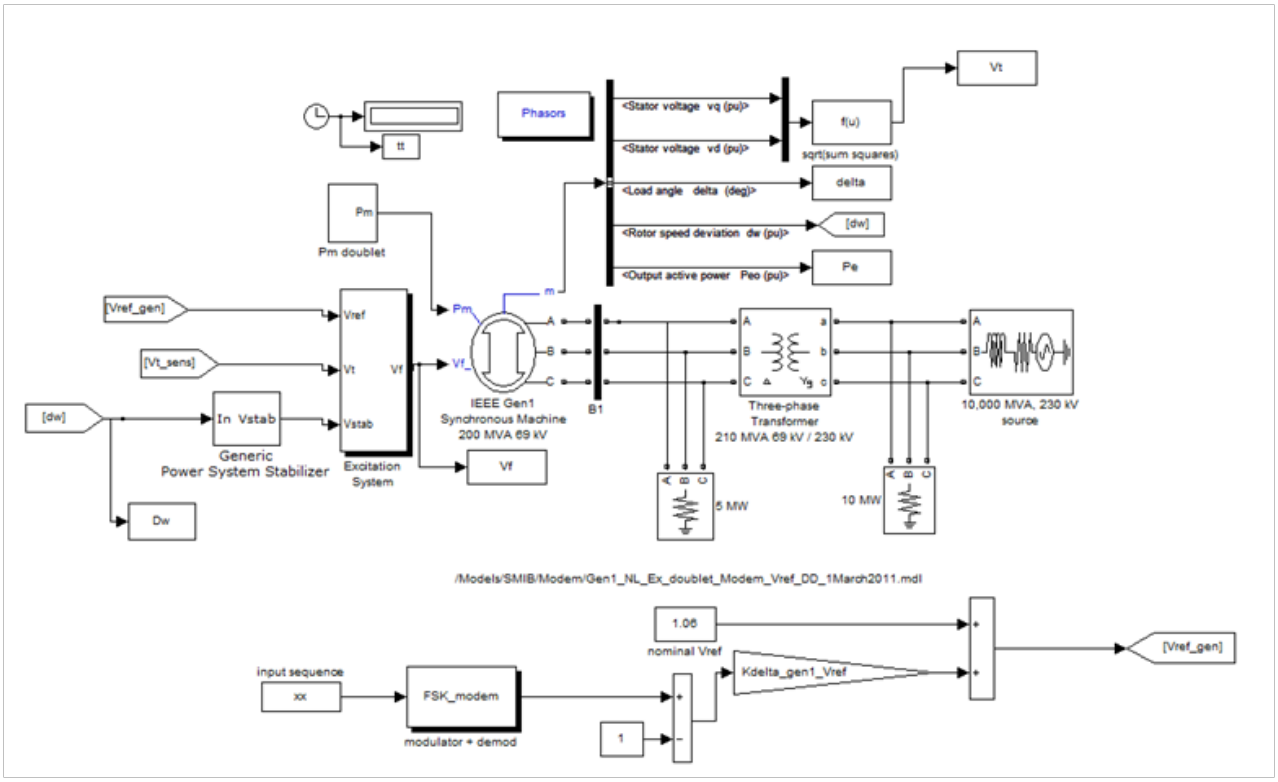


Fig. 4. Single Machine Infinite Bus with FSK Modem Control of Generator Voltage

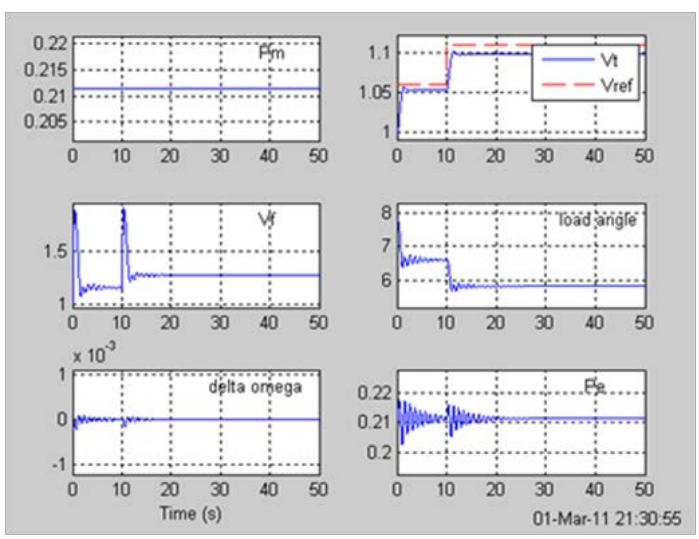


Fig. 5. Simulation Results for Step Change in Generator Voltage via FSK Modem

A remotely controllable circuit breaker is shown in Fig. 6. This consists of a physical model of the circuit breakers, one for each phase, a control input, and an interface to the information/communication network. This controllable breaker is implemented in a load control application in Fig. 7. An input from a control algorithm is provided to the FSK modem which transmits the control signal over a communication link to the circuit breaker. This example is being utilized to control demand response remotely. In addition, future work will utilize a similar physical model to control SVCs as shown in Fig. 3.

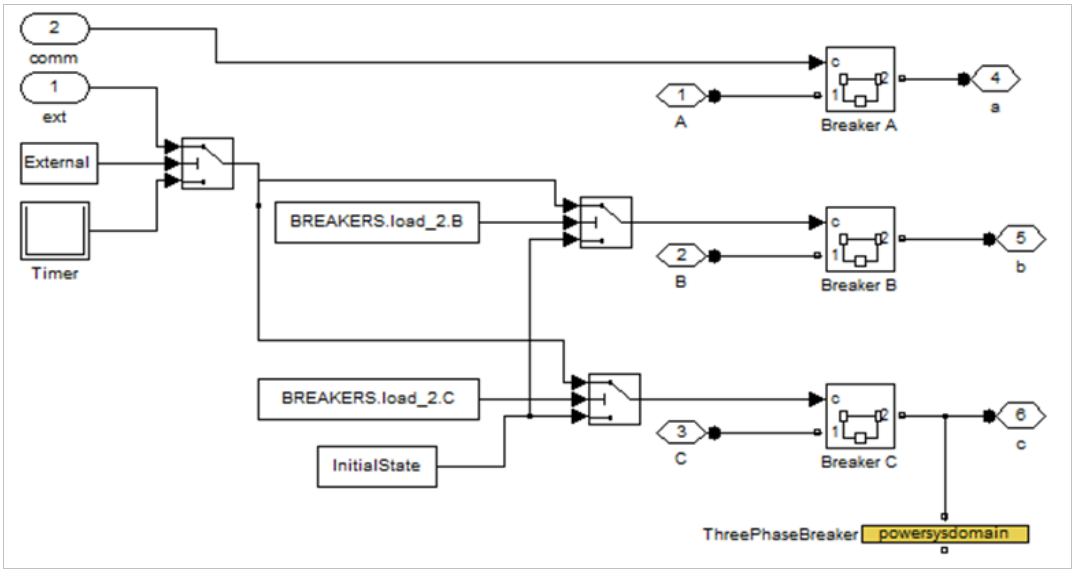


Fig. 6. Model of Remotely Controllable Circuit Breaker

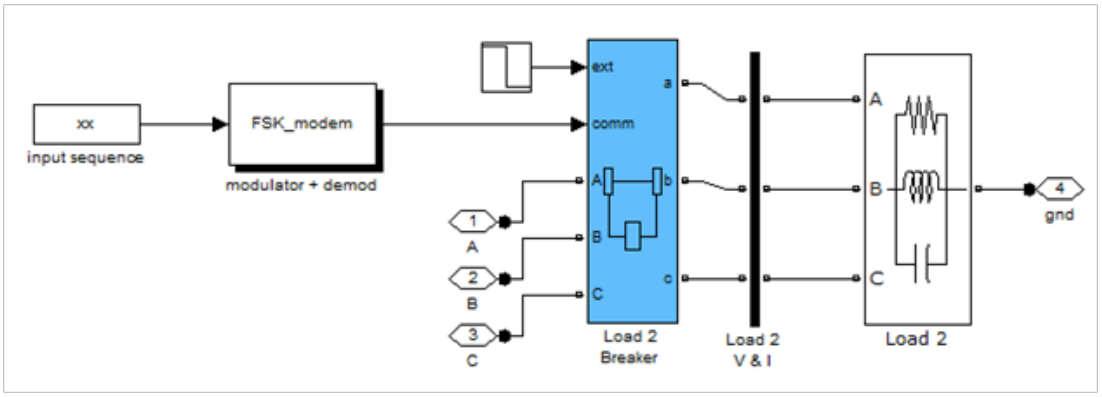


Fig. 7. FSK Modem Controlling Load

Conclusion

This paper presents an approach for modeling smart grid dynamics as a set of interdependent composite networks. The model utilizes an interconnection of communication network, information network, and a power system network to model smart grids with a focus on bulk generation and transmission of power. The resulting model is being used for studying and simulating wide area measurement and control techniques and contingencies of cyber and physical components of the smart grid.

Acknowledgement

This work was supported by the Defense Threat Reduction Agency MIPR# 10-2693M, to the United States Military Academy.

References

[1] N. Jaleeli, et al., "Understanding Automatic Generation Control," IEEE Transactions on Power Systems, vol. 7, pp. 1106-1122, Aug 1992.

[2] D. Trudnowski, et al., "Power-system frequency and stability control using decentralized intelligent loads," Proceedings of the 2006 IEEE Power Engineering Society T&D Conference adn Expo, pp. 1453-1459, May 2006.

[3] S. Chiaradonna, et al., "On a modeling framework for the analysis of interdepenedencies in electric power systems," Proceedings of the 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, 2007.

[4] J. C. Laprie, et al., "Modeling cascading and escalating outages in interdependent critical infrastructures," Proceedings of the 2006 IEEE International Conference on Dependable Systems and Networks, pp. 226-227, 2006.

[5] J. C. Laprie, et al., "Modelling interdependencies between the electricity and information infrastructures," Proceedings of the International conference on Computer Safety, Reliability and Security (SAFECOMP), pp. 54-67, 2007.

[6] P. Crucitti, et al., "Model for cascading failures in complex networks," Physical Review E, vol. 69, Apr 2004.

[7] P. Task Force on Understanding, Mitigation and Restoration of Cascading Failures in Electric Power Systems, "Vulnerability Assessment for Cascading Failures in Electric Power Systems," Proceedings of the 2009 IEEE Power Systems Conference and Exposition, pp. 1-9, 2009.

[8] A. Z. Faza, et al., "Reliability Modeling for the Advanced Electric Power Grid: A Proposal for Doctoral Research," Proceedings of the 33rd Annual IEEE International Computer Software and Applications Conference, pp. 672-675, 2009.

[9] J. Lin, et al., "A General Framework for Quantitative Modeling of Dependability in Cyber-Physical Systems: A Proposal for Doctoral Research," Proceedings of the 33rd Annual IEEE International Computer Software and Applications Conference, pp. 668-671, 2009.

[10] J. Nutaro, "Designing power system simulators for the smart grid: combining controls, communications, and electro-mechanical dynamics," Proceedings of the 2011 IEEE Power Engineering Society General Meeting, pp. 1-5, July 2011 2011.

[11] "NIST Interagency Report 7628: Guidelines for Smart Grid Cyber Security: Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements," 2010.

[12] P. Kundur, Power System Stability and Control. New York: McGraw Hill, 1994.

[13] C. P. Nguyen and A. J. Flueck, "Modeling of communication latency in smart grid," Proceedings of the 2011 IEEE Power and Energy Society General Meeting, 24-29 July 2011.

[14] J. Quintero and V. Venkatasubramanian, "SVC Compensation on a Real-Time Wide-Area Control for Mitigating Small-Signal Instability in Large Electric Power Systems," Proceedings of the 2006 International Conference on Power System Technology, pp. 1-8, Oct 2006.

[15] "MATLAB," http://www.mathworks.com, Ed., ed: The Mathworks, Inc.

Appendix D

Appendix D: A network challenge for situation assessment of command and control

This appendix provides a view of modeling the information dominance problem of military systems as representative of modeling other complex systems. The majority of the information provided here is taken from an earlier paper presented a few years ago at a systems conference.[41] Additional information concerning command and control assessment is taken from a joint paper also presented at a systems engineering conference.[42] The ideas are an extension of earlier efforts to base analysis of information assurance for complex systems on system partitioning into a system of systems. The approach discussed rests upon the notion that the system at hand is intended to achieve some useful purpose and that a system of systems approach provides a feasible methodology for composing the system functionality (behaviors) as an aggregation of sub-systems functionality. Many subsystem processes have continuous process models while higher system models are usually discrete. Composition of components requires consideration of interaction of subsystems, especially when feedback loops are present. A model of Information Assurance (IA) processes consistent with this hybrid system model of complex processes is described. Information dominance is defined as superior situation understanding and superior support for making decisions under uncertainty. The information dominance model is then presented as an extension of the IA model. The appendix concludes with a conjecture that more effective intrusion detection can be achieved by using the known purpose of an information system (e.g. achieving information dominance in support of an operation) to guide allocation of intrusion detection resources.

Index terms – Hybrid Systems, Information Assurance, Information Dominance

Introduction

The phenomenal growth of networked information systems has created significant opportunities for increased efficiencies and associated opportunities for mischief. For military systems, this is reflected in the intent of the United States forces of the future to exploit increased knowledge of friendly and enemy forces (also known as information dominance) and the associated problem increased vulnerability of future forces to deliberate or inadvertent manipulation of friendly and enemy information. For medical systems this is reflected in the expanding capability for monitoring, diagnosing, and predicting patient or group status and

[41] James, J. R., "Modeling of information dominance in complex systems: A system partitioning and hybrid control framework" Proceedings of the 36th Hawaii International Conference on System Science, Hilton Waikaloa, Hawaii, January 2003.

[42] James, John R. and Frank Mabry, "Building Trustworthy Systems: Guided State Estimation as a Feasible Approach for Interpretation, Decision and Action Based on Sensor Data," Proceedings of the 37th Hawaii International Conference on System Science, Hilton Waikaloa, Hawaii, January 2004.

associated concerns related to individual privacy or group discrimination. Similarly, for power, telecommunications, finance or other complex systems, there is an increasing reliance of these critical infrastructure systems processes on networked information systems and associated vulnerabilities to deliberate or inadvertent information systems failures. This appendix presents a view of these complex systems as compositions of systems of systems and proposes a new model of information assurance processes associated with either discrete or continuous system components.

Previous Information Assurance (IA) models have ignored the continuous systems aspects of modeling complex systems. This appendix presents a modeling approach that allows including continuous system models when appropriate.

In this appendix we discuss explicit modeling of the reliability of information maintained on the state of complex systems. The approach discussed for modeling IA components of military systems rests upon the notion that the system at hand is intended to achieve some useful purpose and that a system of systems approach provides a feasible methodology for composing the system as an aggregation of sub-systems. The notions of purpose and system of systems lead to the need to understand the behaviors of the system and its component sub- systems, especially as those behaviors are modified via reactive control to continue meeting the system purpose while reacting to malicious IA activities. Thus, the modeling approach must support capturing process and sub-process behaviors. Maintaining trust of the information being presented is absolutely essential for military planning and re-planning processes and impossible to achieve unless an effective approach for Information Assurance, including risk management is in place.

Organization of the appendix

The next section provides an overview of a modeling framework for analysis of military processes. Military operations depend upon reliable operation of many critical infrastructure processes and the framework discussed is consistent with modeling these infrastructure processes as well as the military processes that depend on their reliable operation. An enterprise architecture is considered to have several views: an operational view of the users, a systems view of the hardware and software implementation, and a technical view of the underlying standards and interoperability protocols. The section has four subsections:

- Operational Architecture
- Technical Architecture
- Systems Architecture, and
- Information Assurance modeling

Section four then extends the modeling framework of section three to consider Information Dominance. Section five discusses resource allocation for intrusion detection and section six summarizes the appendix.

Modeling framework

The modeling framework described here applies the hybrid automaton ideas of hybrid control theory to model military operations. The approach features construction of agents to coordinate interactions of components that are composed to form the system of systems of a force structure planning and executing

a military operation. This approach is general enough to capture the complexity of military operations as well as the interactions of military system components with supporting infrastructure processes. The framework also provides a rigorous way of restricting the set of hybrid trajectories to a collection of discrete and continuous variables. The general approach is mathematically rigorous and, at some point, may support automatic generation of system of systems solutions. However, current tools support the constructive assembly of components of known models into progressively more complex systems of systems and adaptive control of the (well-understood) composed system. This approach also supports development of verification and validation [1] methodologies for a system-of-systems of autonomous enterprise agents since a necessary step in the composition process for composed systems is the satisfaction of independence of components constraints except where feedback loops are allowed. Thus the basic agent in a modeling and simulation framework is a hybrid automaton [2] that is a collection:

$H = (X, V, Init, f, Inv, R)$ where

X is a finite collection of state variables. We assume $X = (X_D \cup X_C)$ with X_D countable and $X_C \in \Re^n$;

V is a finite collection of input variables. We assume $V = (V_D \cup V_C)$ with V_D countable and $V_C \in \Re^n$;

$Init \subseteq X$ is a set of initial states;

$f: \; X \times V \to X_C$ is a vector field, assumed to be globally Lipschitz in X_C and continuous in V;

$Inv \subseteq X \times V$ is an invariant set;

$R : X \times V \to 2^X$ is a reset relation.

We refer to $x \in X$ as the state of H and to $v \in V$ as the input of H.

Associated with this model are rigorous definitions of continuous and discrete states and associated models of continuous behaviors and discrete behaviors and hybrid (combination of continuous and discrete) behaviors. These behaviors consist of continuous, discrete and hybrid trajectories from a set of initial states to a set of final states. The complete power of the hybrid modeling approach is not needed for each component. For some (maybe most) of the components, a discrete model is sufficient. Likewise, for some components, a continuous-system model is sufficient. The hybrid model is used when the composed system has both discrete and continuous components.

The hybrid automaton modeling approach has been developed within the control community for analysis, design and implementation of distributed control systems. The technology enables a more rigorous analysis of the middleware approach for distributed system development whereby applications use well-defined interfaces to access services from other local and distributed applications (the middleware) to provided their own functionality.

The development of military information systems is guided by interacting ideas of purpose and process. For military systems, the purpose is set in the Joint Vision 2020 declaration of achieving information superiority. The process is summarized in the view of the enterprise architecture as the view of a set of interacting architectures described in the Army Enterprise Architecture (AEA) of Figure 1 [3].

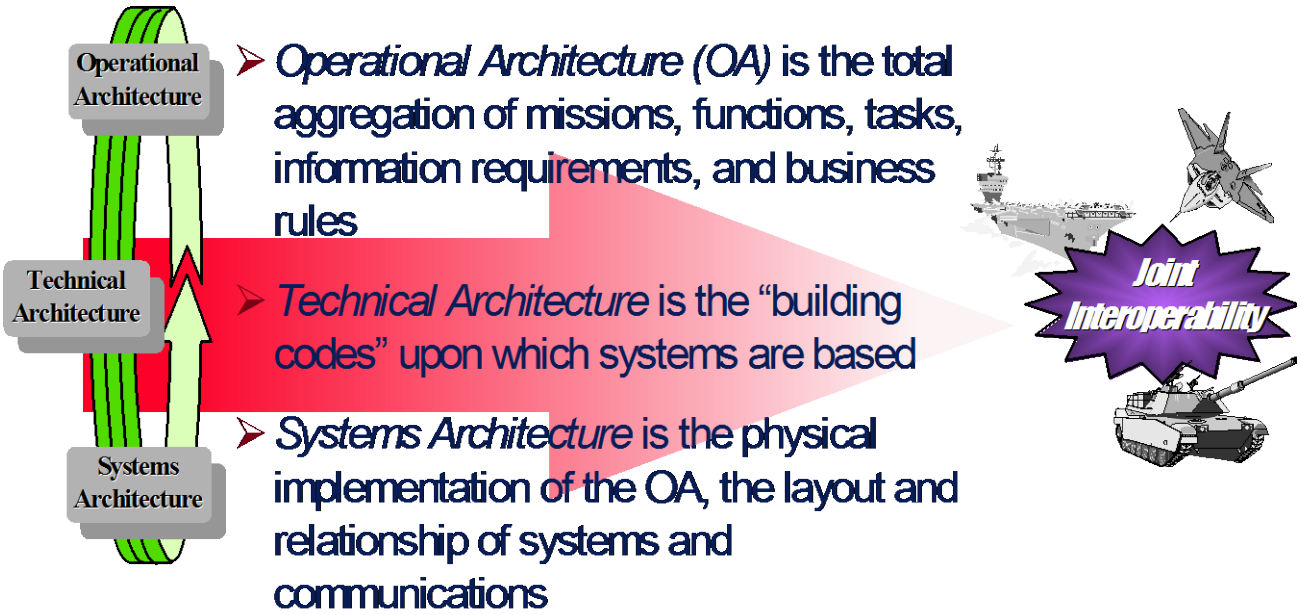


Figure 1. Army Enterprise Architecture (AEA)

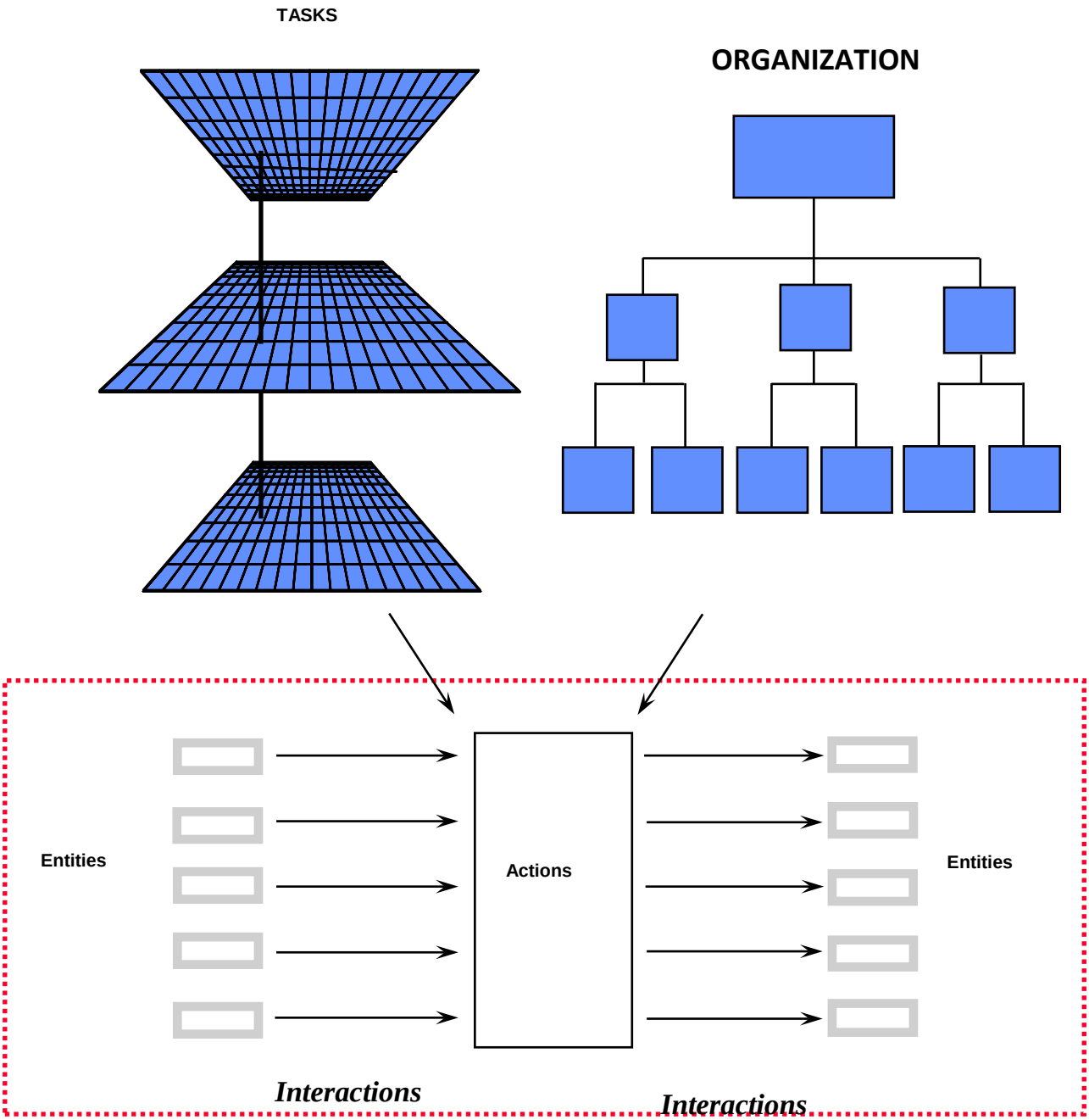


Figure 2. The Conceptual Model of the Mission Space (CMMS) view of an Operational Architecture

Operational Architecture: The Operational Architecture (Figure 2) captures the operational processes supporting the purpose that is captured in the mission statement for a given operation. One way of viewing the elements of the operational architecture is to capture the relationships between the organizational partitioning of the force structure and the functional partitioning of the force structure. An example of this is the Conceptual Model of the Mission Space (CMMS) approach (see Figure 2) that has

been developed by the Defense Modeling and Simulation Office (DMSO). The basic idea is to provide a crosswalk between the functional partitioning of tasks (functional entities) to be performed at each level in a hierarchical structure and the force structure components (physical entities) that take actions to accomplish the functional tasks. Our system state identification problem is then to filter the observed signals into appropriate sets of data for the unit being analyzed and to compare known patterns for separable components to patterns observed in the data being analyzed. Unit entities take actions to achieve behaviors needed to cause the current system state to move to applications. The Department of Defense technical architecture takes this approach, which is similar to the layered approach taken by the Open Systems Interconnection (OSI) model for modeling distributed networked systems.

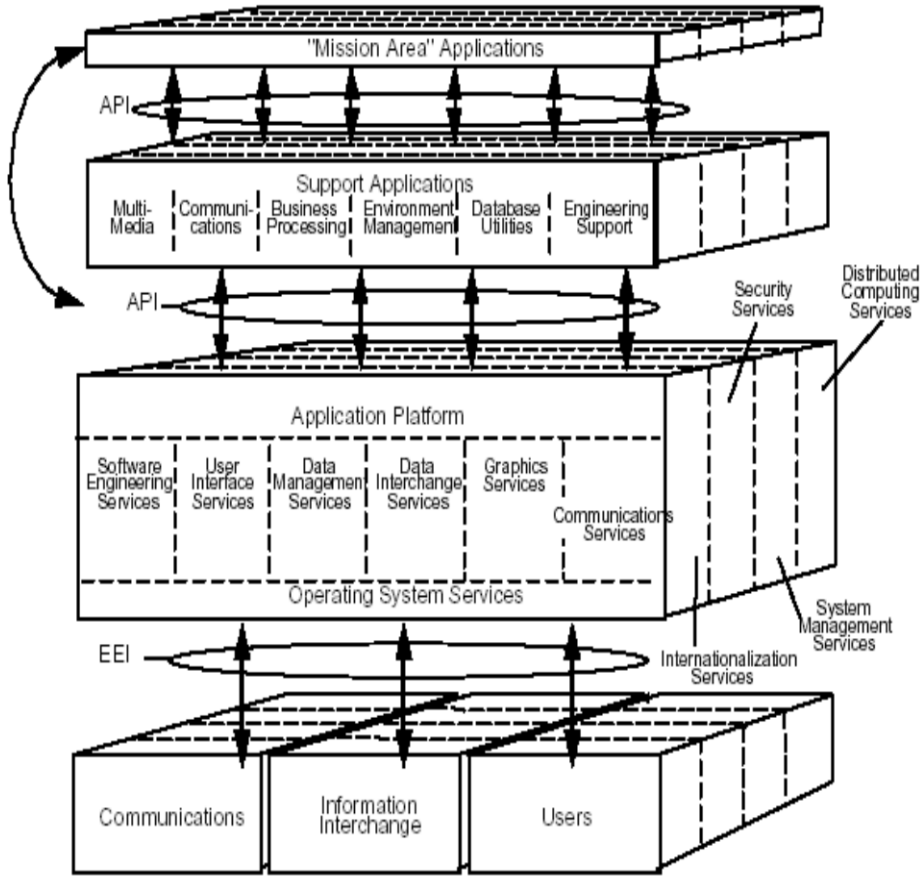


Figure 3. The Technical Architecture

The Army Technical Architecture for Information Management (TAFIM) Technical Reference Model (TRM) [4] is shown in figure 3. The TAFIM TRM organizes software into two entities, an Application Software Entity and an Application Platform Entity. The Application Software Entity communicates with the Application Platform Entity through an API. The Application Platform Entity communicates with the external environment through the External Environment Interface (EEI). The TAFIM TRM decomposes these entities into subcategorizes as shown in Figure 3. Currently, these ideas are expressed as a set of specifications for the Defense Information Infrastructure Common Operating Environment (DII – COE). The various mandates of the DII-COE establish the operating system and communication system constraints for interconnecting defense information systems.

Systems Architecture

A Systems Architecture (SA) is a description, including graphics, of the systems and interconnections providing for or supporting a warfighting function. The Army systems architecture for Force XXI envisions support for both installation applications and force structure applications. A high-level SA view is shown in Figure 4 and provides a summary of relationships between strategic, operational, and tactical information systems, including the links envisioned between installation (fixed) and tactical (mobile) networks.

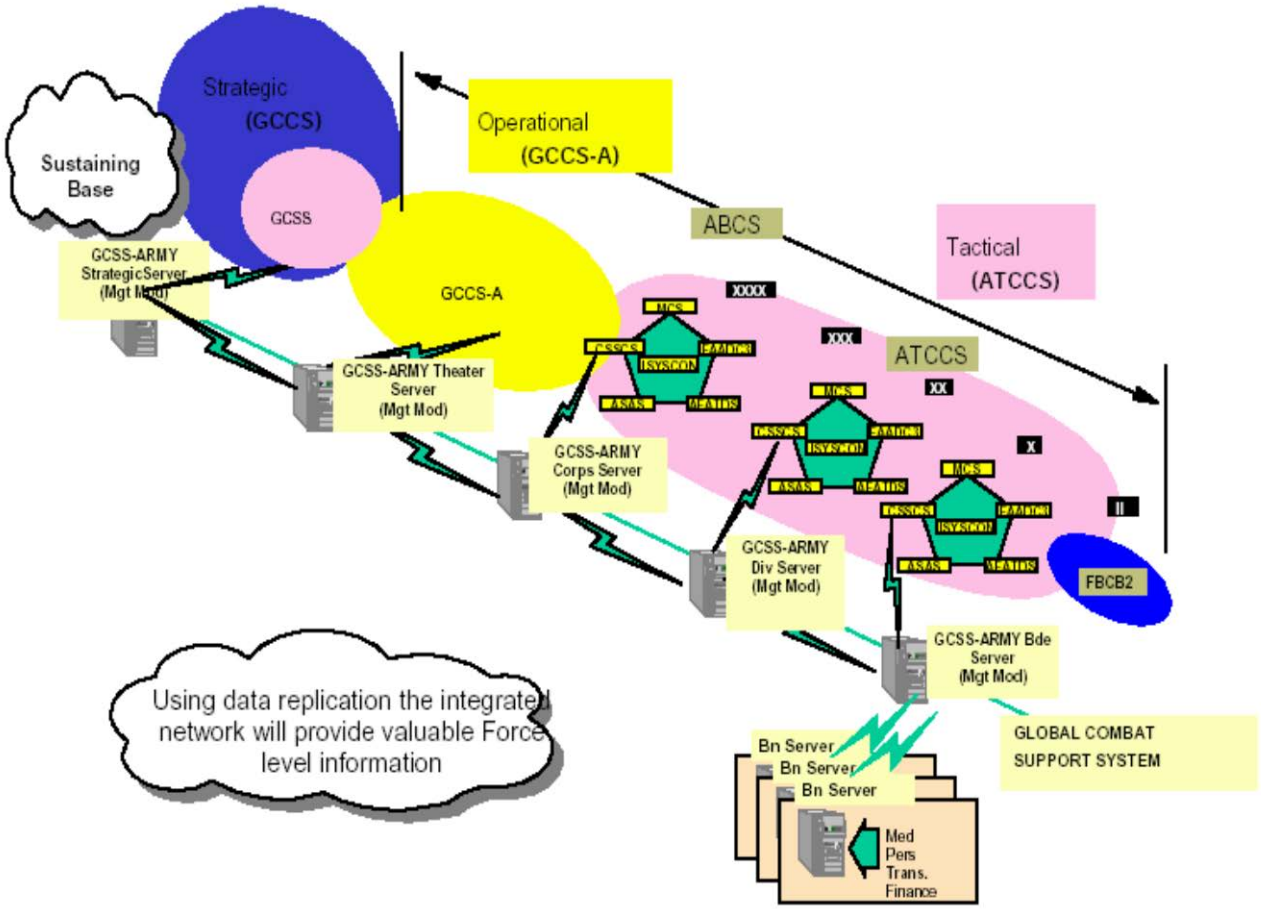


Figure 4. Command and Control Systems From Strategic Through Tactical Level

A low-level SA view in shown Figure 5 and provides an overview of administrative/logistics and command and control networks in an armor company. In Figure 5, the command and admin/log nets are voice, single-channel radio systems with limited range (i.e. they are frequency-modulated (FM), line-of-sight radios) with capability of limited data transmission. The Extended Position Location Reporting System (EPLRS) portion of the Future Battle Command, Brigade and Below (FBCB2) system provides situation awareness at company level through automatic dissemination of position information as well as automatic distribution of other selected information (e.g. selected activity and status information).

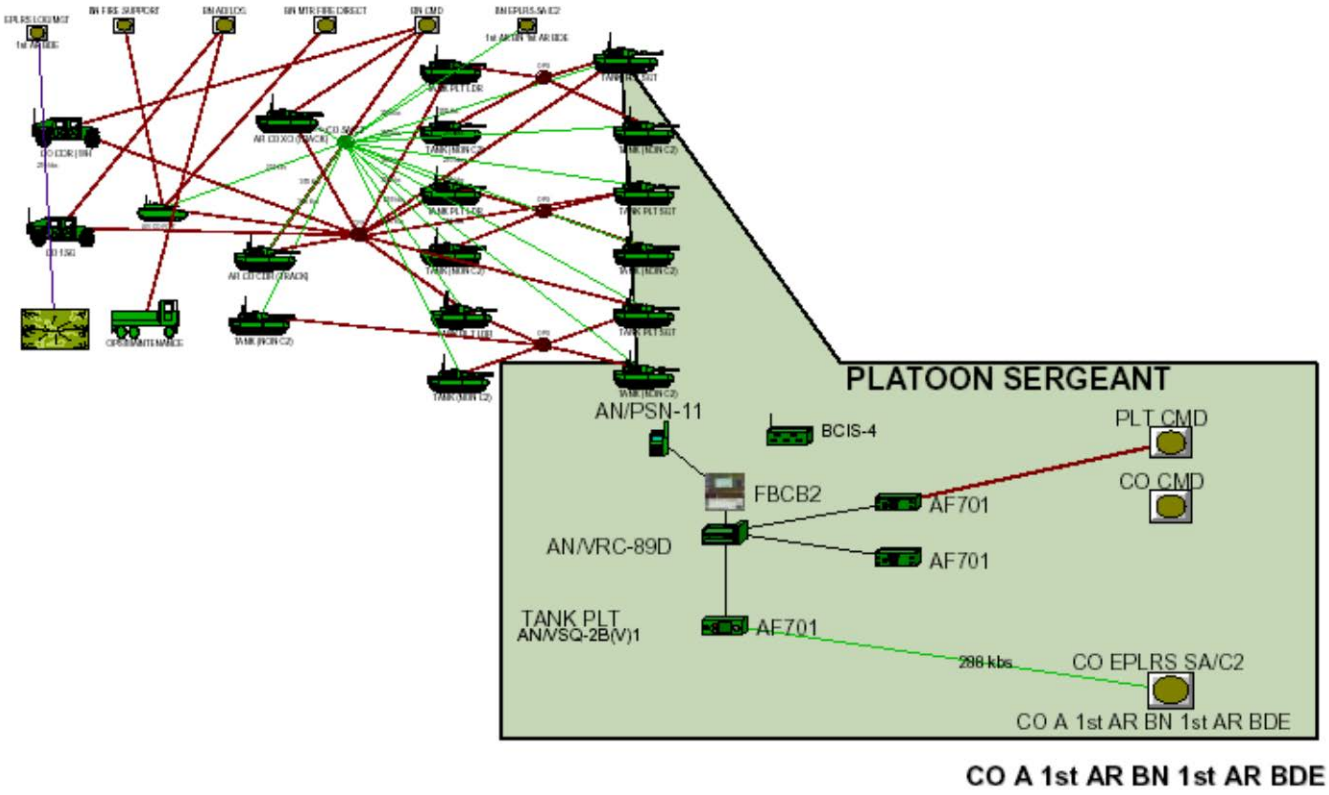


Figure 5. Administration/Logistics and Command/Control at the Company/Platoon Level

While armor companies do not have organic multichannel radio systems, Patriot batteries do have a Mobile Subscriber Equipment (MSE) Small Extension Node (SEN) multi-channel radio system. Major changes to current communication systems will occur when the Warfighter Information Network –Terrestrial (WIN-T) and Joint Tactical Radio System (JTRS) are fielded. WIN-T and JTRS will enable more flexible achievement (more widespread use) of tactical internets during joint force operations.

Information Assurance Modeling for Military Systems

Current ideas for reacting to malicious network activity apply fundamental ideas of control system science to consider the ideas of feedback loops and reactive control to compensate for anomalous events due to malicious activity. These ideas are based on the observation that a protection activity is often based on a sequence of sense, decide, act as a means of adapting to new circumstances. Adaptive network security is advocated by Internet Security Systems [5], a prominent provider of commercial products for network security, as a necessary approach for securing commercial enterprise networks against malicious attacks. ISS recommends a Detect, Monitor, Respond sequence for managing network attacks. Since military communication architectures are deliberately designed to change over time, degradation and enhancement

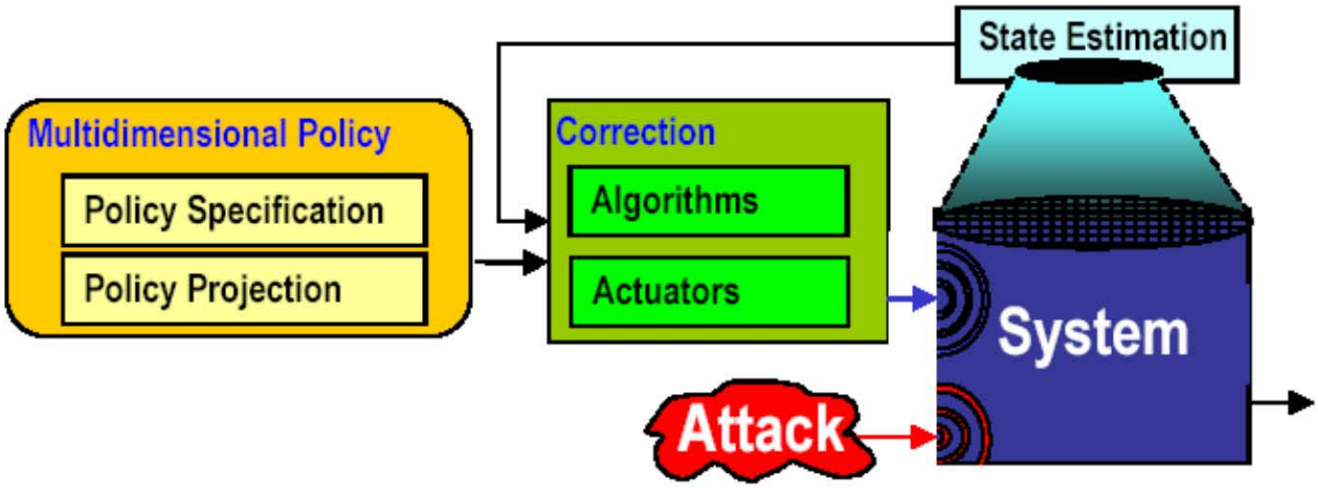


Figure 6. Feedback control concept for Autonomic Information Assurance

of network information processing capability over time will be a characteristic of unit operations. Consistent with the discussion of the preceding paragraph, a unit's ability to detect, monitor, and respond to IO attacks should be based on: a risk assessment of unit vulnerabilities, a deliberate decision concerning an acceptable level of risk [6], and methodologies to achieve that level of risk in unit information systems.

For example, a detect, monitor and respond capability is a necessary element of the Autonomic Information Assurance [7] project of the Defense Advanced Research Projects Agency (DARPA). The AIA project envisions a reactive capability to respond to an IO attack (see Figure 6) predicated on an ability to estimate the current state of the battlefield processes being monitored.

Given that military information systems are planned to evolve over time in synchrony with the changes of the force structure and the missions being executed, and also given the fact that the system itself is expected to change under attack, the Information Assurance Model must support this evolutionary process. The minimal capabilities include estimating (detecting) the current system state, comparing the current

state to a desired state (monitoring), and selecting an appropriate response (reacting) when the system deviates "too far" from the desired state. A model that supports this set of modeling requirements is shown in Figure 7.

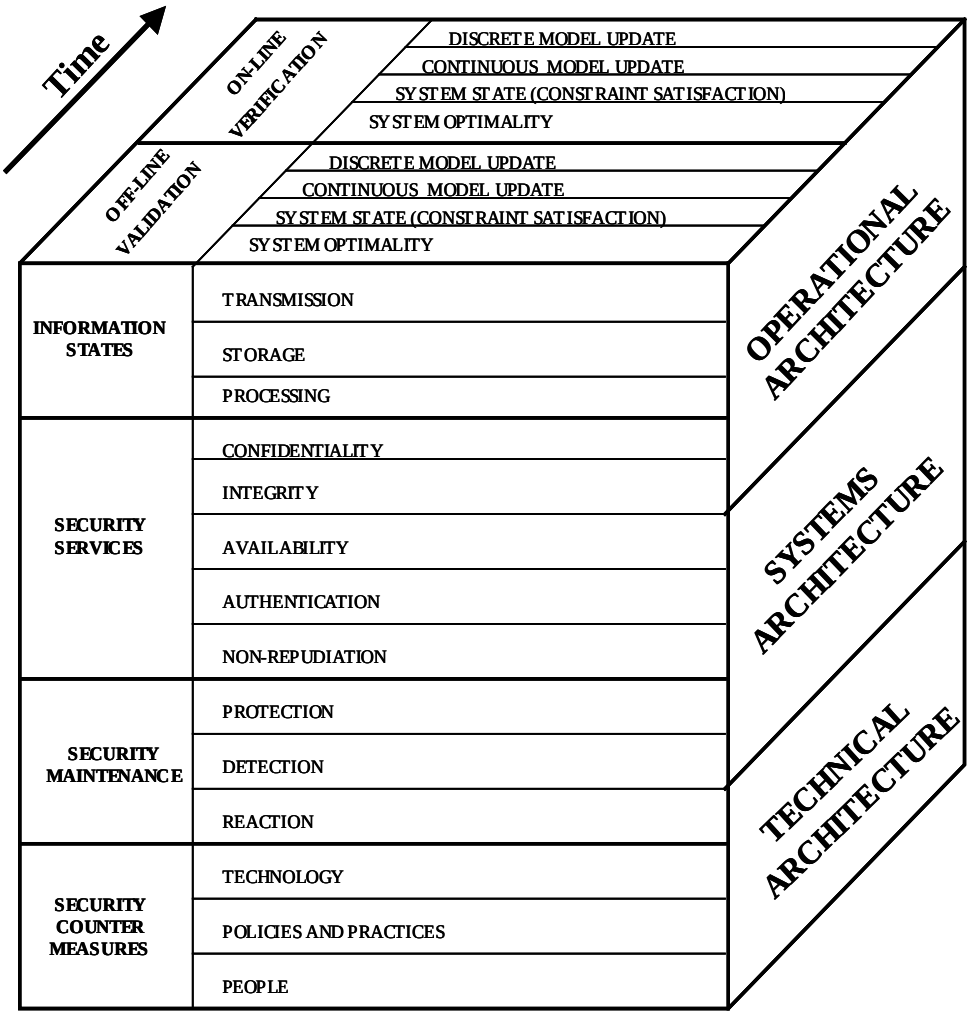


Figure 7. A model of Information Assurance processes for providing Security Services

The Information Assurance Model of figure 7 includes the ideas of discrete-event models previously proposed but also adds the ideas that these models may have both continuous and discrete system states and that these models change over time through a verification and validation process which explicitly supports changing the model in compliance with the constraints of the operational, technical, and systems architectures. As indicated in a recent paper in modeling Information Assurance, the original model of John McCumber [8] to capture Information security (INFOSEC) modeling requirements was later extended by him to accommodate the Canadian Trusted Computer Product Evaluation Criteria (CTCPEC). The work of Maconachy et al. [9] extends McCumber's work and addresses the problem that, in their words, "INFOSEC has evolved into Information Assurance (IA). This is more than a simple semantic change … In today's information intensive environment, security professionals have expanded the scope, and thus the understanding of information and systems protection under an umbrella term referred to as IA." The model of Maconachy et al. includes the Information States, Security Services, and Security Countermeasures of Figure 7 and also the notion that these entities change over time. This Information Assurance Model of Figure 7 is a modest extension of the work of Maconachy et al. to add the notion of Security Maintenance (the sense, decide, act idea of reactive control) and to explicitly consider

some verification and validation mechanism to enable specification, analysis, design, implementation, test, and maintenance of Security Services in the context of system purpose which enables construction of some optimality criterion for use in deciding how to evolve the system.

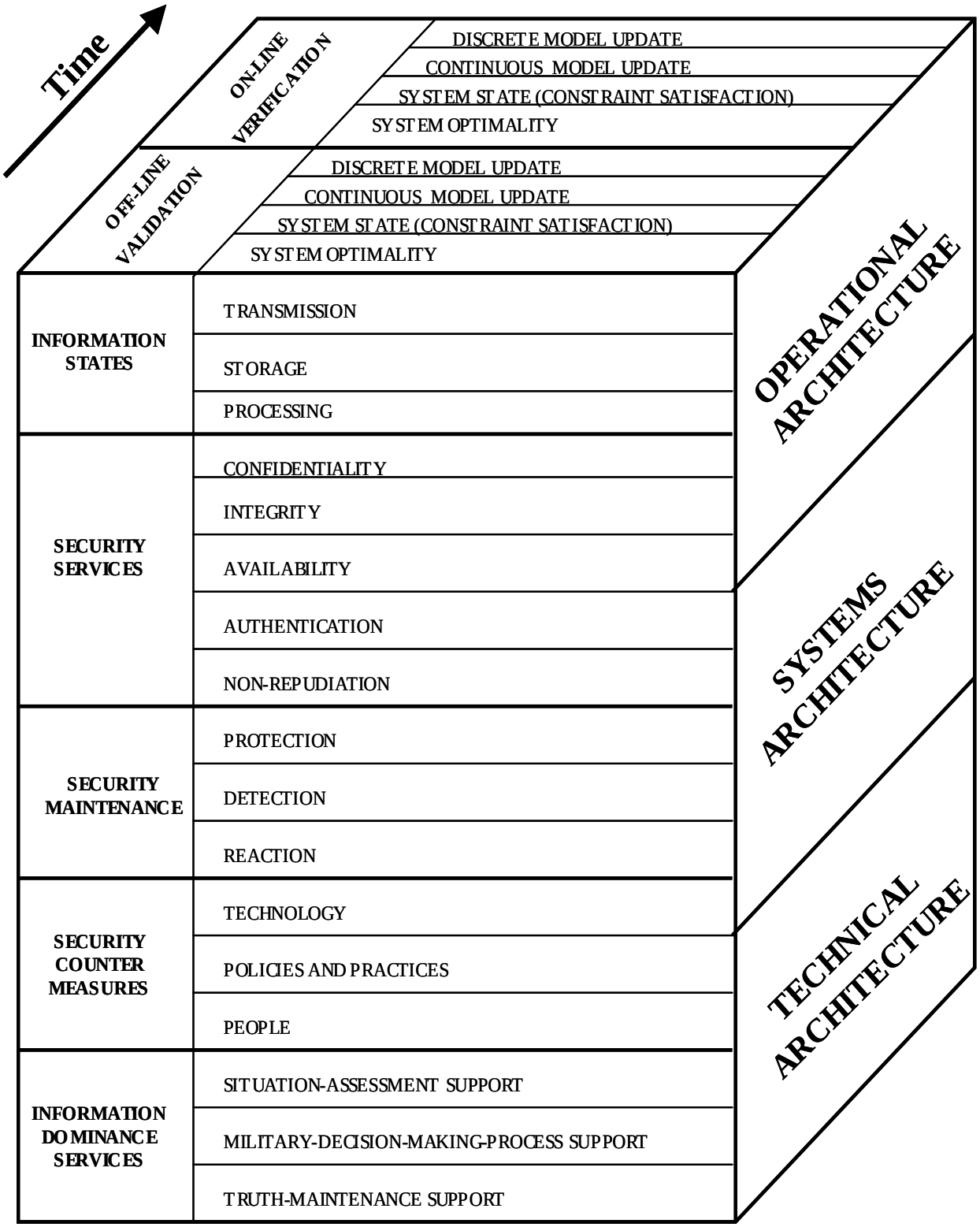


Figure 8. Modeling Information Dominance Processes

Information Dominance Modeling

Information dominance involves use of superior battlespace knowledge and superior decision making capability to achieve the goal of consistently "getting inside the decision cycle" of opposing forces. Thus, we define Information Dominance in terms of three essential services to achieve this goal: situation-assessment support, military-decision-making-process support, and truth-maintenance support. Dominance in each of these services is needed in order to consistently and reliably "get inside the decision cycle" of adversaries. It should be noted that lack of dominance in any one of these three services may render dominance in the other two useless in terms of meeting the goal of enabling commanders to "see the battlespace" better than opponents and apply that knowledge to more effectively command friendly forces by making better decisions under uncertainty than opposing force commanders. Thus, a slight extension of figure 7 results in the model of information dominance processes represented in figure 8.

A conjecture for resource allocation

This section provides a conjecture that more effective intrusion detection can be achieved by using the known purpose of an information system (e.g. achieving information dominance in support of an operation) to guide allocation of intrusion detection resources.

Conjecture

The conjecture is stated in the form of cost-based allocation of intrusion detection resources to maintain acceptable levels of risk that enterprise knowledge has been compromised. The underlying assumption is that malicious activities will be deliberately concentrated in a manner reasoned to degrade achieving system purpose so that an effective use of available resources would be to focus detection activities upon those intrusion techniques that support that end.

The notion is that:

- There is a value chain of information based on support for enterprise processes,
- There is an associated increase in entity value in moving up the value chain from data to knowledge,
- Knowledge varies from enterprise to enterprise,
- Conjecture: Intrusion Detection will be more effective if explicit efforts are made to allocate Intrusion Detection Resources to support efforts to maintain acceptable levels of risk that enterprise knowledge has been compromised

Military Example:

- For the military, a value chain that has high-priority is the set of events that result in authorization to use deadly force

- For the military deadly force is largely applied by officers in the Navy and Air Force and by units for the Army and Marines (i.e. officers make the decision to engage in the Air Force and Navy while soldiers in units make decisions to engage in the Army and Marines)

- Information Assurance resources (including Intrusion Detection resources) should be allocated to maintain an acceptable level of risk that application of deadly force to support meeting the commander's intent has not been compromised

- The conjecture rests upon the assumption that a knowledgeable enemy will concentrate malicious activities upon those friendly assets most useful to meeting the commander's intent which is the purpose for use of deadly force

Say there is some metric for determining degree of attainment of system Purpose:

- Completely attained
- More than Adequately Attained
- Adequately Attained
- Less than Adequately Attained
- Minimally attained.

Then, to the degree that measures are available to indicate closeness to achieving system purpose and also that measures are available for estimating the relative contribution that elements in a knowledge value chain make to achieve the system purpose, then a cost-based allocation of resources can be made to protect, in priority, those assets which contribute the most to completion of enterprise purpose.

Military Example continued:

Consider the value chain associated with applying deadly force to achieve the commander's intent for the operation outlined in Figure 9.

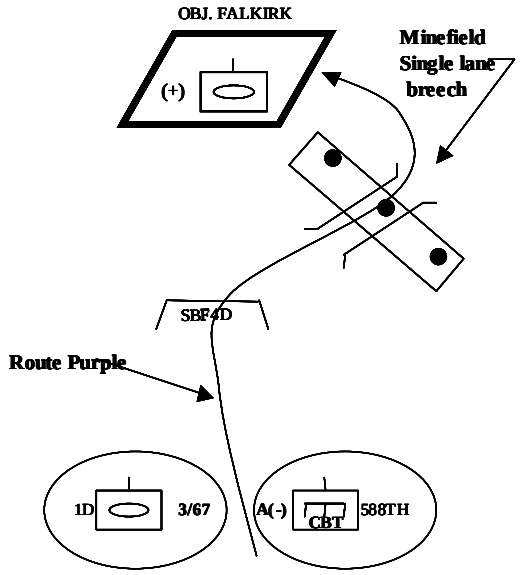


Figure 9. Battalion Attack to Seize Objective

Currently, an Army Brigade (about 4000 soldiers) is the level at which the information systems represented by Figures 4 and 5 are integrated. The companies (about 100 soldiers) of an Army Battalion (about 500 soldiers) use the communications equipment shown in Figure 5 to automatically share situational awareness data and to implement required analog and digital communication networks.

Figure 9 summarizes the Battalion Commander's intent to seize objective Falkirk. The graphic constraints for this portion of the operation indicate that D Company of 3rd Battalion, 67th Armor will attack along Route purple, occupy Support By Fire Position 4D and provide covering fire for an element of A Company 588th Combat Engineers to make a single-lane breech of a minefield. Company D will then

conduct a passage of lines of the engineer element and continue the assault along Route Purple to seize objective Falkirk. Not shown is a diversionary supporting attack by another Company of 3/67 Armor.

One top-level partitioning of information system components is into two sets: one set for those sub-systems associated with administration and logistics and one set for those sub-systems associated with force-level control (command and control).

Information value chains for different phases of an operation Prior to commencement of the attack, those Battalion-level systems that enable administration and logistics functions have a relatively high priority since the forces will not be ready to achieve the commander's intent unless they are fully manned by trained and qualified personnel operating the required sets of equipment.

As the time for commencing the attack draws close, those Battalion-level information assets that allow commanders and staffs to understand the current locations and activities of friendly and enemy forces (i.e. the intelligence estimation assets of force-level control) will have a relatively high priority.

Once the attack begins, those Battalion-level information systems that enable force level control functions will have a relatively high priority. The force-level control functions are those that position the company (15 tanks) and platoon (four tanks) elements for application of deadly force as well as those systems that coordinate requests for supporting fire. Deadly force is applied by the combat-crew (tank) level and by supporting fire elements (mortars, artillery, aircraft, …). The Army uses a synchronization matrix to summarize the activities required by different force structure elements during different phases of an operation. The synchronization matrix provides a means for constructing metrics to estimate whether subordinate units of a given unit have met time and spatial constraints for achieving a commander's intent. Thus, by phase and unit by echelon, we can estimate if goals are being: completely attained, more than adequately attained, adequately attained, less than adequately attained, or minimally attained.

The joint force information presented in different contexts to different individuals should address the needs of the user. This is particularly true in the case of engagement decisions where the different views of the common operational picture should reflect the fact that engagement decisions are made primarily by officers in the Air Force and Navy and primarily by combat weapons crews in the Army and Marine Corps. Estimates of the relative importance of different information system elements will require on-line identification of system state since the information system architecture (like the force structure it supports) will change as an operation proceeds. Changes will occur at the network level, at the middleware level, and at the application level.

Summary

We have discussed modeling the information dominance problem of military systems as representative of modeling other complex systems. The approach discussed rests upon the notion that the system at hand is intended to achieve some useful purpose and that a system of systems approach provides a feasible methodology for composing the system as an aggregation of sub-systems. Many subsystem processes have continuous process models while higher system models are usually discrete. Composition of components

requires consideration of interaction of subsystems, especially when feedback loops are present. A model of Information Assurance (IA) processes consistent with this hybrid system model of complex processes was described. Information dominance was then defined as superior capability in situation understanding and making decisions under uncertainty. The information dominance model was then presented as an extension of the IA model.

References

[1] John James and Dave Barton "A Framework for Verification and Validation of Integrated and Adaptive Control Systems" Proceedings, 11th IEEE International Symposium on CACSD, Anchorage, Alaska, September, 2000.

[2] John Lygeros, George Pappas and Shankar Sastry "An Introduction to Hybrid System Modeling, Analysis and Control" Preprints of the First Nonlinear Control Network Pedagogical School, pages 307-329, Athens, Greece, 1999.

[3] Office of the Director of Information Systems for Command, Control, Communications, and Computers (ODISC4), The Army Enterprise Architecture Master Plan, Vol.1, 30 September, 1997.

[4] Department of the Army, Joint Technical Architecture – Army, Version 5.0, 11 September 1997.

[5] Internet Security Systems, Adaptive Network Security Handbook, http://www.iss.net/ .

[6] Department of the Army, Field Manual FM 100-14, "Risk Management," Washington, DC, 23 April1998.

[7] http://web-ext2.darpa.mil/body/procurements/old_procurements/isojan00.html

[8] McCumber, John. "Information Systems Security: A Comprehensive Model". Proceedings 14th National Computer Security Conference. National Institute of Standards and Technology. Baltimore, MD. October 1991.

[9] W. Victor Maconachy, Corey D. Schou, Daniel Ragsdale and Don Welch, "A Model for Information Assurance: An Integrated Approach" proceedings of the 2001 IEEE Workshop on Information Assurance and Security United States Military Academy, West Point, NY, 5-6 June, 2001

Appendix E

Appendix E: Army Common Operating Environment Architecture[43]

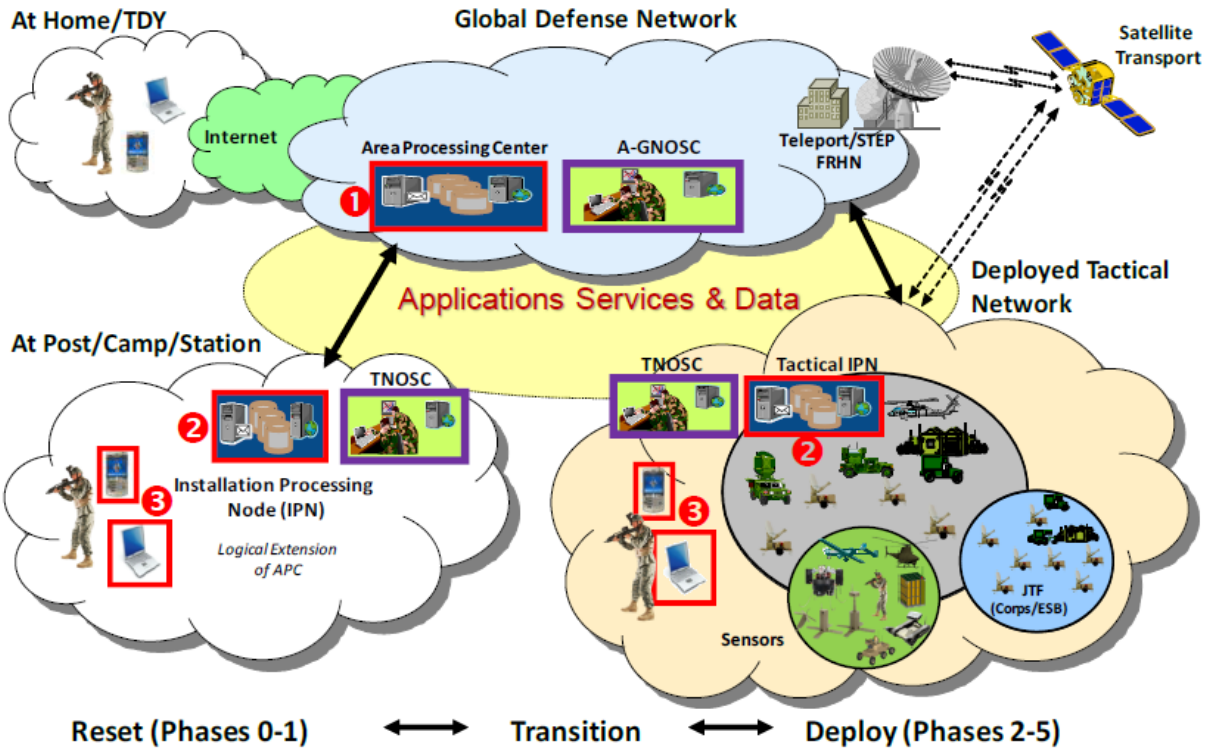


Figure C1 - Army Enterprise Network (LandWarNet)

The following items are included in this document's scope.

❶**Area Processing Centers in the Global Defense Network:** In support of the Federal Data Center Consolidation Initiative, the Army is consolidating data centers into Area Processing Centers (APCs). APCs deliver enterprise services on an area and theater basis from a limited number of standardized, centrally managed facilities connected to the Defense Department's global high-speed backbone network. APCs also host functional applications (e.g., Battle Command Common Services (BCCS), business, intelligence) for use by operating and generating forces. APCs not only centralize Army, Joint and coalition data, applications and services, but also support a

[43] Army Common Operating Environment Architecture, Appendix C to Guidance for 'End State' Army Enterprise Network Architecture, http://ciog6.army.mil/LinkClick.aspx?fileticket=udbujAHXmK0%3D&tabid=79

worldwide DoD intranet by which a single connection allows a user to access these resources from anywhere, at any time, in any operational environment.

❷ **Tactical Installation Processing Nodes (IPN):** Forward-deployed forces are provisioned instances of high-performance computing, storage or enterprise services in order to meet mission-specific performance requirements. BCCS is currently designated as the Tactical IPN. It enables host capabilities for SharePoint and web development in a service-oriented infrastructure[1]. Additionally, the Battle Command Server provides interoperability services, including Publish and Subscribe Services and the Data Dissemination Service. The server also supports convergence with the U.S. Marine Corps by providing a data exchange gateway that allows the direct exchange of Common Operating Picture data.

❸ **End-User IT Devices for Operational Forces:** Tactical and non-tactical end-user IT devices include mobile devices and client computers.

Appendix F

Appendix F: Seeing the Real World: Sharing Protected Data in Real Time[44]

Summary

We describe a new capability for "owners" of protected data to quickly and securely share real-time data among networked decision-support and real-time control devices with whom the "owners" of the data have explicitly decided to "share" the data. The service is based upon implementation of a recent formal definition and mathematical result (James et al. 2009) derived from the decades-old Bell-LaPadula information security result (Bell and LaPadula, 1973). The service provides decision makers a means of securely and automatically sharing critical information across security barriers based upon declaration of sharing policies. The declaration and implementation of information sharing policies based upon a need-to-share has been shown to be compatible with information protection policies based upon a need-to- know. Indeed, the implementation of the need-to- share service is based upon extending the mathematical foundations of need-to-know information security systems (the Bell-LaPadula result of 1973).

Introduction

The flowing valued information (FVI) project is a three-year project supported by the Army Research Office (ARO) to investigate scientific barriers to sharing information among coalition partners involved in counter-insurgency (COIN) operations and nation- building efforts1. The FVI project has developed a support service termed Need To Share (NTS) (James et al., 2009). This service allows groups to share information with each other (at the group level) in a secure manner via a repository service. An IATT (interim authority to test) request for operation of this software on the Defense Research and Engineering Network (DREN) network at USMA has been approved for a test in the Summer of 2011 to share data among the National Military Academy of Afghanistan (NMAA) in Kabul, Afghanistan, the United States Military Academy (USMA) at West Point, New York, and the Royal Military Academy Sandhurst in Surrey, England. A student capstone engineering project at West Point (Lanahan, 2011) has built a user-friendly interface to enable "owners" of information to share desired data and to designate whom the data is to be shared with. Additionally, extensions to the basic capability are being built (Huggins et al., 2011) to implement the service on smart phones and other mobile devices. This paper summarizes the formal result which forms the basis for the information sharing service and provides details concerning real-time extensions of the existing service. The next section provides an overview of the formal result and the following section describes the existing service. We then describe the real-time extensions and conclude the paper with a summary section.

[44] J. James, F. Mabry, and K. Huggins**, Seeing the Real World: Sharing Protected Data In Real Time**, Proceedings of the Hawaii International Conference on System Science (HICSS 2012), January 4-72012, Maui, Hawaii.

Formal Extension of the Bell-La Padula result

The original Bell-LaPadula result was based upon general systems theory available at that time. The primary distinction to be discussed in this paper is the extensions necessary to formally consider real-time systems. That is, while Bell and LaPadula considered a system in its most general form to be a relation on abstract sets, the modern system theorists add consideration of continuously-varying systems as well as compositions of discrete, set-based, systems and continuous systems. Functional concepts of a mapping from one state space (the domain) to another (the range) remain the same. While Bell and LaPadula considered the system S to be a relation on the abstract sets X and Y, Lee and Varaiya (and others) consider the general system S to have elements which are members of abstract sets and also elements which are members of general functional spaces (Lee & Varaiya, 2002). The mathematical details of the extensions to the Bell-LaPadula model are too lengthy to be provided here. However, the mathematical details are available on-line. The on-line report provides mathematical details on (1) extending the models of the systems being analyzed to include what are described today as "complex systems" and (2) extending the existing Bell-LaPadula model for defining a failure to secure information (a security compromise) to include defining a failure to share information (a sharing compromise).

The mathematical result follows current system theory (Lee and Varaiya, 2002) results in modeling and analyzing systems which are compositions of logical and continuous system components. Associated with the current systems theory models are rigorous definitions of continuous and discrete states and associated models of continuous behaviors and discrete behaviors and hybrid (combination of continuous and discrete) behaviors. These behaviors consist of continuous, discrete and hybrid trajectories from a set of initial states to a set of final states. The complete power of the hybrid modeling approach is not needed for each component (and may not be desirable!). For some (maybe most) of the components, a discrete model such as that used by Bell and La Padula is sufficient. Likewise, for some components, a continuous-system model is sufficient. The hybrid model is used when the future states of the composed system includes parameters of interest which exhibit both discrete and continuous behaviors (evolutions). We are convinced that for our particular problem space (decision support systems and real-time control systems), the hybrid model is generally required for capturing the range of parameter values of interest for complex system evolution. Our problem space of interest in this paper is that which can adequately represent tactical-level military operations where success in humanitarian assistance/disaster recovery (HADR) operations requires reasoning about trustworthiness of information elements to be flowed between distributed information nodes in a manner which (1) increases the value of information available for goal-oriented decisions in accordance with the intent of the commander taking into account that some of the information elements vary continuously with time and space, and (2) which complies with a command decision to share information.

It is interesting to note that addressing item one above (flowing valued information) was a subject of discussion at the time the creators of the original Bell-La Padula model were working on their model (Bell D. E., 2005), (Landwehr, Heitmeyer, & Mclean, 1984), (Denning, 1976), at least in terms of seeking to analyze information security in terms of information flow. While this paper seeks to extend the framework

of Bell and La Padula in terms of a formal treatment of general systems modeling and information sharing, we remark that the implementation details, in addition to following the Bell-LaPadula extensions in terms of information security and sharing, will also be achieved as extensions to the current military messaging systems in terms of information flow between network nodes. As indicated by John McLean, there has long been considerable interest in fashioning the treatment of security in the same manner as Shannon had done for information theory by establishing the science for determining channel capacity (McLean, 1990). McLean's treatment of information flow considers bi- directional flow of information as preserving security for causal systems if the security state of the information object of interest is considered at different instances of time. However, McLean's treatment does not consider continuous values in time and space and also does not consider the case in which information value decays over time or distance from where it is most useful. Bell's review in 2005 of the Bell- LaPadula model states: "Consideration of access modes led to the unexpected identification of a hard-to- name information flow property, the star property. The relation W that conceptualized allowable changes of state was not constructive and was therefore insufficient for the analysis and formulation of core system calls that change the security state. (Bell D. E.,2005)" The star-property refers to the basic constraint of information flow across a security level in the Bell- LaPadula model as allowing "no read-up, no-write- down" operations (Figure 1 and Figure 2 of Bell D.E., 2005). Thus, decision support tools available to commanders today continue to rely on security models which restrict analysis to parameters whose values are members of sets. This restriction does not enable reasoning about parameters of interest whose values change continuously.

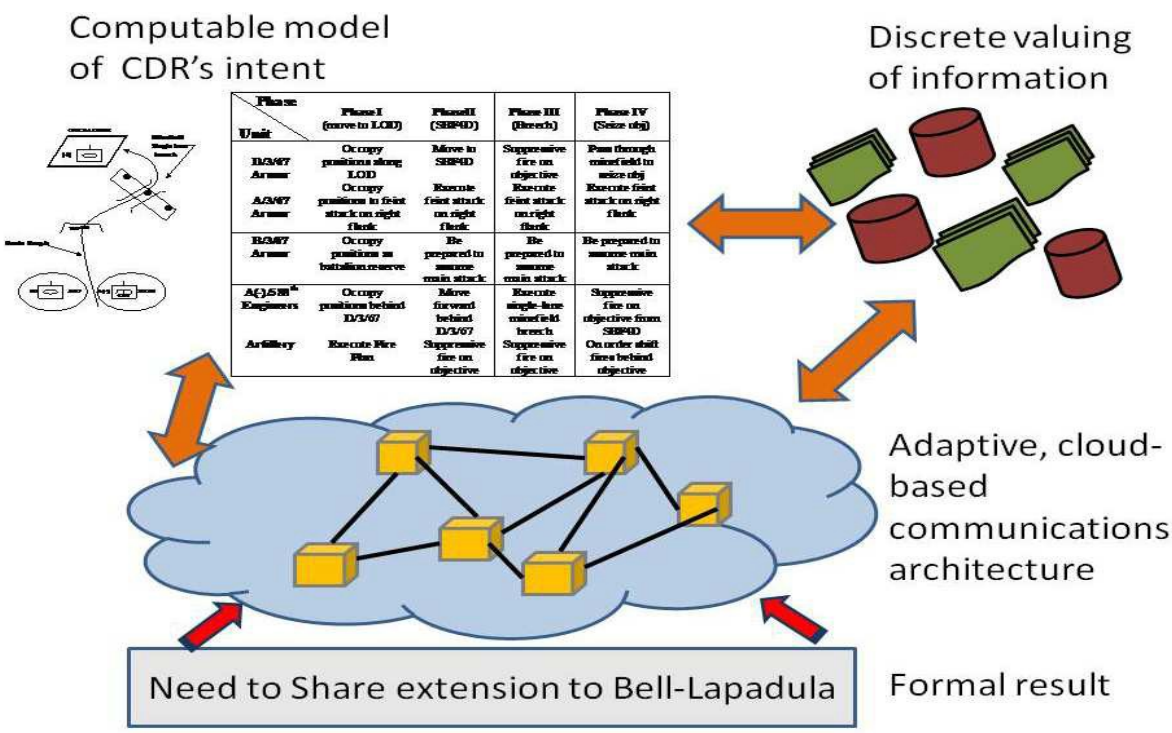


Figure 1. The need to share project

Description of the Existing Service

Figure 1 provides an overview of the Need To Share project. The underlying assumption of the Need To Share project is that a computable model of command intent is captured by the widely-used military abstraction of a "synchronization matrix" shown in the upper left of Figure 1 and associated map graphics which constrain unit movement. The entries in the synchronization matrix are descriptions of unit activities at different times (operational phases are matrix columns) and at different locations (unit components are matrix rows). The long range goal of the project is to value information at different nodes in a communication architecture based upon the relative utility of meeting command intent and to move information among nodes to increase the value of information available to make command and control decisions. The nodes of interest include nodes in a military command and control network, communication nodes used by local government and non-government agencies, and nodes used by other coalition partners in humanitarian assistance and COIN operations. For COIN operations in Afghanistan, a current barrier to achieving General Petreaus' information sharing goal of "understanding the people" is that information available in military networks and other associated government and non-government networks cannot cross information security barriers associated with the various networks. In the case of united States forces, even though government policy is that commanders at any level can declare a need to share information with government and non-government entities, current information system implementations do not provide support for automatically sharing information with entities who are not authorized to be "on the net" used by the military commander. As shown in Figure 1, our result provides a means for sharing information among nodes in a cloud-based communications architecture which, for military operations, can include nodes which are not "on the net" with other military units. Our initial implementation, described below, is moving sensitive but unclassified (SBU) information among nodes on the United States Defense Research and Engineering Network (DREN) and other communication nodes on the Internet. Figure 2 provides a summary of a representative process for selecting information to share.

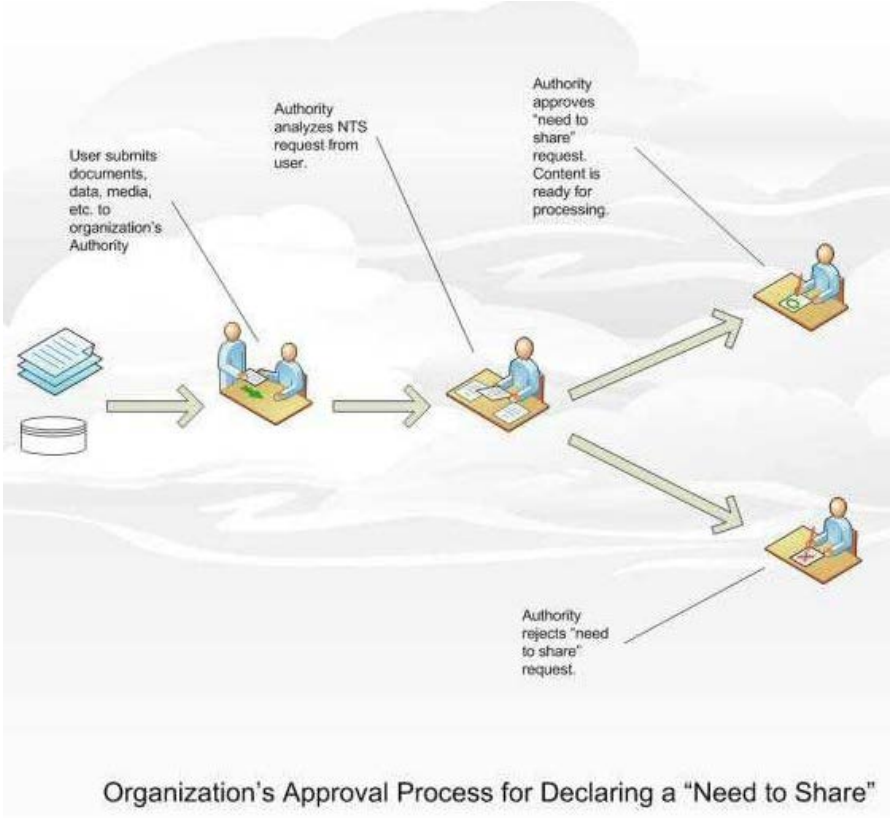


Figure 2. Selecting information to share is an organizational process

Content placed in the repository is encrypted and signed. Only those groups "trusted" to have access to any specific set of data can open the encrypted form. When data is received in this manner, the first step in processing the data is to verify that the data was electronically signed by another group member. NTS member groups each have an "authority" who provides a public key that is available to each of the other authorities for encryption and authentication of NTS data. The repository can reside on a single commonly accessible node or be realized as a service accessed as a "cloud computing" service. FVI-NTS provides support for movement of static content (in the form of files and directory structure) with no "file type" constraints. The basic software supporting encryption and signing uses the OPENSSL software suite (the November 2009 version is FIPS 140-2 certified). Figure 3 provides a summary of the method implemented for encrypting the information to be shared with selected users and groups.

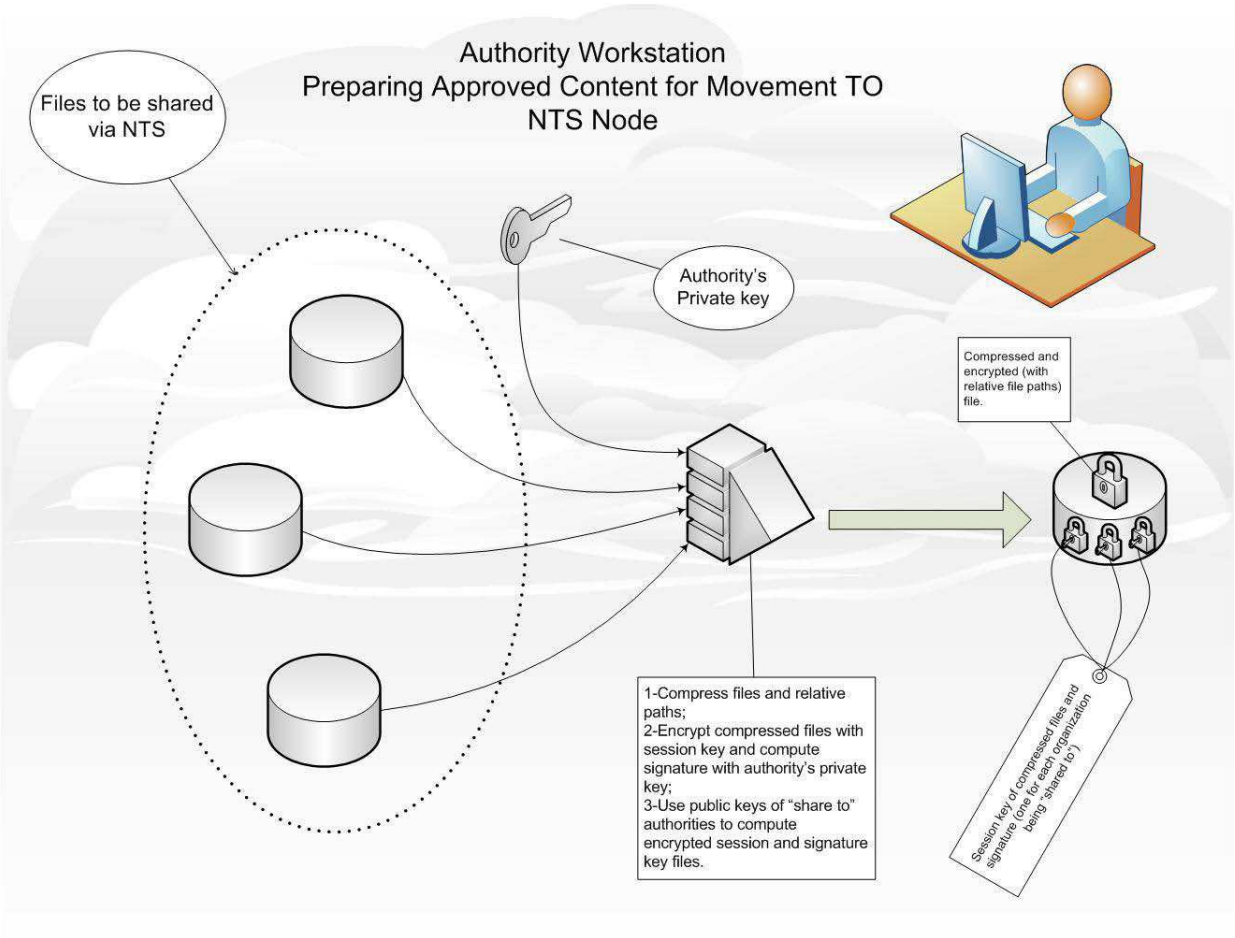


Figure 3. Preparing the data for sharing is achieved by a designated authority

The method depends upon implementation of some approach for generating and maintaining address lists and associated public and private keys for encrypting and decrypting the shared data. We refer to this as a Master Basic Trust Certifier (MBTC). The FVI-NTS system follows a 5-step protocol for sharing information

among clients in the cloud. These steps are request, aggregation, transport, decomposition, and consumption.

1) Request: When a user in an organization desires to share information (Figure 2), such as documents, media, data, etc, she must submit it to the organization's 'Authority' that analyzes the information and either approves are rejects the request. The 'Authority' (Figure 3) can be a person or an automated system.

2) Aggregation: When an outgoing set of files has been reviewed and accepted for sharing by the 'sending' organization's authority, the data is aggregated in preparation for transport. There are six sub-steps in the FVI-NTS protocol that accomplish this task.

1. The set of files to sent are compressed (including any relative sub-paths) into a ZIP file.
2. The ZIP file is encrypted with a randomly generated symmetric key.
3. For each node that files are being shared with, the symmetric key (generated in step 2) and the digest signature of the encrypted ZIP files are encrypted with the public key for the receiving authority. The file is then saved with the encrypted ZIP file (from step 2). The name of the encrypted key file is that of the node being "shared to." An encrypted key file is also generated for sending node (with its name).
4. For each node that is not being shared with, an encrypted key file is written but the symmetric key value used is zero (which never occurs otherwise).The set of files to be sent are compressed (including any relative sub-paths) into a ZIP file.
5. The set of encrypted key files and the ZIP files are saved to a directory named initially "Txxxxxxxxxxxxx" where xxxxxxxxxxxxx is replaced with the millisecond accurate clock on the authority's workstation.
6. After all the files have been copied to the local node, the directory is renamed with the initial "T" removed. [Note: only new directories without an initial 'T' are processed by receiving NTS authority workstations. Should an RSYNC capture a directory that has not been 'finalized' it will not be processed until a subsequent RSYNC occurs and renames the directory.]

3) Transport: After the files have been collected and encrypted, the authority the moves the set of files to the local node. At that point, the data is copied to the other nodes in the cloud (Figure 4). Each local node will have a directory of directories that acts as the repository of files to be sent or just received.

4) Decomposition of files to be shared with other members of the NTS group of organizations. RSYNC will only copy new content to other nodes. All content on each node is encrypted. Each node has the needed keys to run RSYNC (within a SSH tunnel session) on each of the other nodes. No authority's private or public keys are ever stored on a node. Should a node's file contents ever become accessible to anyone outside the group of authorities participating in the 'need to share' group the content will remain 'secure' from inappropriate access. At the receiving end of the node cloud architecture, the tasks are the same, but simply reversed. The node authority will move the interested zip file (or files) off the node onto the local network.

5) Consumption: On the local network, the authority will use his public key to decrypt the ZIP file and proper disperse the files within his/her organization. Central to this design is the existence of a party acting as the Master Basic Trust Certifier (MBTC) that provides the access certificates on each node for the

other nodes (thus allowing SSH-RSYNCH based communication). The MBTC also communicates the public keys of the authorities to each of the other authorities. The individual authorities for each organization can use OPENSSL software to generate their public and private keys. The MBTC does need to know the public or private keys of any of the authority workstations. What encrypted content the members choose to move is obscured from the view of the MBTC. A specific MBTC can provide the management of the NTS group of nodes without ever having access to the actual content being transmitted. It should be noted that this architecture provides a solution to the end node problem, where an un-trusted, individual computer becomes part of a trusted, network. The data that is stored on each node is encrypted and essentially inaccessible to any node except for the intended receiver (See Figure 4.). As a result, there is no issue with a network -managed need to trust (i.e. the new end-node can only provide encrypted data to a network node which has chosen to accept the data from the new end node so some trust process has occurred and future trust activities can be among nodes can be monitored and controlled by the network controllers as desired). Any computer that joins the FVI-NTS cloud, however, must first obtain the proper keys from the MBTC.

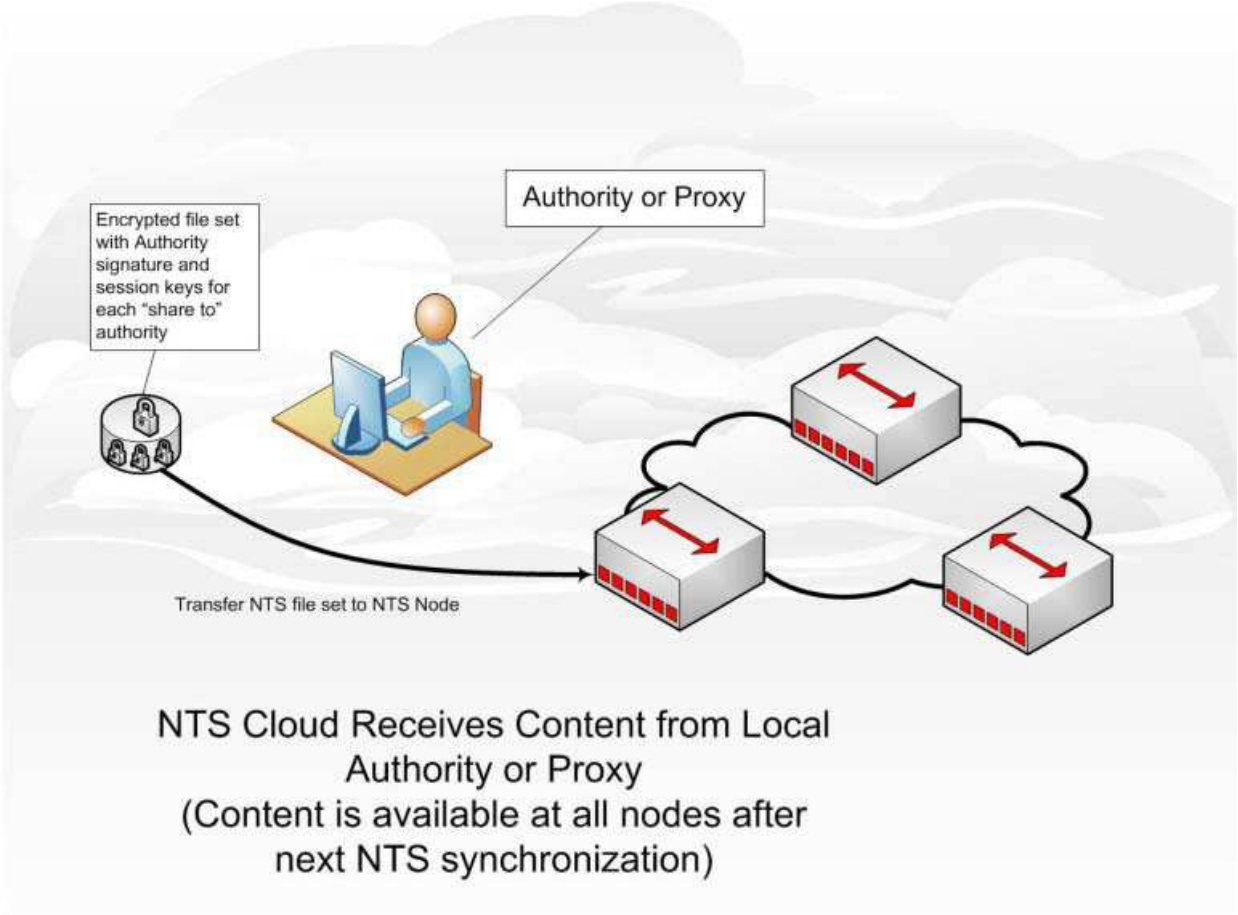


Figure 4. Sharing information among nodes in a communication network

Real-time extensions

While the work to date on FVI-NTS provides support for the trusted sharing of systems of files, it is strictly static in form. Operation of many systems generally necessitates the availability of real-time content (James and MCClain 1999, James and Mabry, 2004). Operation of many systems also frequently requires that information being transmitted be shared with only those trusted to receive it. For example, one challenge in enabling cooperative control of the smart grid in the United States is the requirement for an assumption of distrust among the operators of the various segments of the power grid in the United States (James , Dodge, Graham and St Leger , 2009) which played a minor role in the last cascading power failure in the United States and Canada.

Beginning with the concepts addressed in developing FVI-NTS, an additional operational form is being developed that supports need to share real-time streaming data. The same infrastructure concerns and guarantees are used to provide a service that allows multi-cast content to be shared from real-time sensing sensors or information sources in highly encrypted form for use by those "trusted" to receive it. The technical system supports segmented transmission of binary content that begins each segment with the encryption key for the following data transmitted in an encrypted manner using each trusted group's public key. Only members trusted to receive the content can decrypt a copy of the session key for the following segment. At the end of each segment sending group's private key is used to compute a signature for the preceding segment. This content is included in the encrypted portion of the segment. Any group receiving and decrypting the segment can then use the public key of the group sending the content to verify that there has been no modification of the content of the segment during transmission. Once a segment beginning is located the multi-cast content can be decrypted very quickly and its authenticity evaluated at the end of the segment. While the encryption overhead will be such to prohibit the sharing result in fast control loops present in telecommunications control and faster control loops, the sharing result will be usable in real- time decision support systems as well as in slower control loops such as chemical process control, water treatment facilities, or pipeline control systems.

The length of the segment directly controls the maximum amount of data that may be received that could be tampered with before a trusted recipient would detect such tampering. Because the public keys are shared among the groups participating in the NTS partnership, there is no network based traffic to check credentials of the other parties. At the next received segment boundary any trusted member can begin decrypting the NTS-Real-Time (NTS-R) multi-cast stream. At present a fixed, pre-negotiated segment is used. Again, this avoids any additional network negotiation or transmission of information for what is a fixed body of service information and content. In order to minimize overhead, member groups of an NTS partnership may be incorporated into one or more federations who are provided the same shared private key for those trusted to receive the content on the basis of federated membership. Only an individual group (not a federated set of groups) can provide an NTS-R source. Information being used to sense critical and sensitive information can be provided to any recipients trusted to receive the information. Any other party "listening" to an NTS-R stream can (at most) use the stream as a source of "white noise" but cannot determine any portion of the actual content included in any segment or the stream. At each segment's start, a new decryption key is generated and then encrypted using the public key of each trusted group or

federated set of groups, single public key. Note: the transmitting group may not be a member of one or more of the federated groups that they are providing content to. As such a transmitting node may not be able to decrypt its own transmission. The code is available for anyone interested in testing the current implementation, http://www.netscience.usma.edu .

5. Conclusion

We have described an extension and a formal result for a well-known information security result. These new results have enabled implementation of an approach for sharing protected information across security barriers in real-time. We have provided an overview of the mathematical underpinnings to the result as well as a discussion of an initial implementation of the approach for static information sets. We have described the current extensions to the initial implementation which support real-time sharing of information to overcome existing barriers to construction of decision support and real-time control of large-scale distributed systems which require sharing of information among different control systems which are distributed in time and space. Such control systems occur repeatedly in coalition efforts for security activities in COIN operations as well as in cooperative control of large- scale distributed system such as power grids, transportation systems, and gas pipelines. The service provides decision makers a means of securely and automatically sharing critical information across security barriers based upon declaration of sharing policies. The declaration and implementation of information sharing policies based upon a need-to- share has been shown to be compatible with information protection policies based upon a need-to- know. Indeed, the implementation of the need-to- share service is based upon extending the mathematical foundations of need-to-know information security systems.

6. References

[1] Aubin, J. P. (1991). Viability Theory. Cambridge, MA: Birkhauser Boston Inc.

[2] BAST, Board on Army Science and Technology. (2005). Network Science. Washington DC: National Academy Press.

[3] Bell, D. E. (2005). Looking Back at the Bell-La Padula Model. Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC 2005) (pp. 337-351). IEEE Xplore.

[4] Bell, D. E., & LaPadula, L. (1973). Secure Computer Systems: Mathematical Foundations - Volume I. Mitre Technical Report 2547 .

[5] Denning, D. E. (1976). A lattice model of secure information flow. Communications of the ACM, Volume 19, Number 5, May 1976 , 236-243.

[6] Deshpande, A., & Varaiya, P. (1995). Viable Control of Hybrid Systems. In P. Antsaklis, W. Kohn, A. Nerode, & S. Sastry, Lecture Notes In Computer Science; Vol. 999, Hybrid Systems II (pp. 128-147). London, UK: Springer-Verlag.

[7] Foley, S. (1989). A model for secure information flow. Proceedings, 1989 Symposium on Security and Privacy (pp. 248-258). IEEE.

[8] Gong, L. (2009). Java Security: A Ten Year Retrospective. Proceedings, 2009 Annual Computer Security Applications Conference. Honolulu, HI: Conference Publishing Services.

[9] Honda, K., & Yoshida, N. (2007). A uniform type structure for secure information flow. ACM ACM Transactions on Programming Languages and Systems (TOPLAS), Volume 29, Issue 6 .

[10] Huggins, Kevin, Frank Mabry, and John James, "Flowing valued information based on a need to share," First IEEE International Workshop on Network Science, West Point, NY June 2011.

[11] James, J. R. (2000). Thoughts on Information Operation Detection as a Nonlinear, Mixed-Signal Identification Problem: A Control Systems View. Proceedings, 2000 IEEE Symposium on CACSD (p. 6). Anchorage, Alaska: IEEE.

[12] James, J. R., & Mabry, F. (2004). Building Trustworthy Systems: Guided State Estimation as a Feasible Approach for Interpretation, Decision and Action Based on Sensor Data. 37th Hawaii International Conference on System Science (p. 6). Kohola Coast, Hawaii: HICSS.

[13] James, J. R., & McClain, R. (1999). Tools and Techniques for Evaluating Control Architecture. Proceedings,10th IEEE International Symposium on CACSD (p. 6). Kohala Coast, Hawaii: IEEE.

[14] James, J., Dodge, R., Graham, J., & St. Leger, A. (2009). Gap Analysis for Survivable PCS: Final Report. I3P, http://www.thei3p.org/publications/ResearchReport14.pdf.

[15] James, John R., Frank Mabry, Kevin Huggins, Michael Miller, Thomas Cook, Florian Tamang, Sam Abbott- McCune, Howard Taylor and William J. Adams. Secure Computer Systems: Extensions to the Bell-La Padula Model. West Point, NY: USMA Network Science Center. December, 2009

[16] Lanahan, Justin T., Allen Latty and Rodravian Murray, "Need To Share - Flowing Valued Information and Secure Networking," First IEEE International Workshop on Network Science, West Point, NY June 2011.

[17] Landwehr, C. E., Heitmeyer, C. L., & Mclean, J. (1984). A Security Model for Military Message Systems. ACM Transactions on Computer Systems, Vol. 2, No. 3, August 1984 , 198-222.

[18] Lee, E. A., & Varaiya, P. (2000). Introducing Signals and Systems, The Berkeley Approiach. First Signal Processing Education Workshop. SPE.

[19] Lee, E., & Varaiya, P. (2002). Structure and Interpretation of Signals and Systems. Addison-Wesley.

[20] Lygeros, J., Pappas, G., & Sastry, S. (1999). An Introduction to Hybrid System Modeling, Analysis and Control. Preprints of the First Nonlinear Control Network Pedagogical School, (pp. 307-329). Athens, Greece.

[21] McLean, J. (1990). Security Models and Information Flow. 1990 IEEE Symposium on Security and Privacy. Oakland, : IEEE Press.

[22] Ross, R., Katzke, S., Johnson, A., Swanson, M., & Stoneburner, G. (2008). NIST SP800-39, Managing Risk from Information Systems An Organizational Perspective. Gaithersberg, MD: NIST, http://csrc.nist.gov/publications/drafts/800-39/SP800-39-spd- sz.pdf.

[23] Ross, R., Swanson, M., Stoneburner, G., Katzke, S., & Johnson, A. (2004). Guide for the Security Certification and Accreditation of Federal Information Systems. Gaithersberg, MD: NIST Special Publication 800-37, http://csrc.nist.gov/publications/nistpubs/800-37/SP800-37- final.pdf.

[24] Thompson, K. R. (2006). "GENERAL SYSTEM" DEFINED FOR PREDICTIVE TECHNOLOGIES OF A- GSBT (AXIOMATIC-GENERAL SYSTEMS BEHAVIORAL THEORY). IIGSS Academic Publisher: Scientific Inquiry, vol. 7, No. 1, 10.

[25] Tse, S., & Zdancewic, S. (2007). Run-Time Principals in Information-Flow Type Systems. ACM Transactions on Programming Languages and Systems, Vol. 30, No. 1.