A Systems Engineering Approach To Information Assurance Operations

Dr. Raymond J. Curts, CDR, USN (Ret.)
Strategic Consulting, Inc.
5821 Hannora Lane
Fairfax Station, VA 22039-1428 USA
(703) 395-9143
email: rcurts@erols.com

Dr. Douglas E. Campbell, LCDR, USNR-R (Ret.)
Syneca Research Group, Inc. (www.syneca.com)
600 Maryland Avenue, S.W., Suite 695
Washington, D.C. 20024 USA
telephone: (202) 741-2124 fax: (202) 554-2903
email: dcamp@syneca.com

Abstract

Systems engineering is the branch of engineering concerned with the development of large and complex systems, where a system is understood to be an assembly or combination of interrelated elements or parts working together toward a common objective. Past experience has shown that formal systems engineering methodologies have not always been successfully applied to large and complex information systems. Complex information systems are commonplace in Command and Control (C2) operations. The ability to build, operate and maintain such systems is crucial to the effectiveness of C2. Most importantly, an Information Assurance (IA) program must surround these systems on a global scale across multiple, joint, allied, inter-related platforms. In this paper, the authors will demonstrate why a systems engineering approach is best suited for large and complex information systems, as well as the overall information assurance operations that must also reside with these systems.

1.0 INTRODUCTION

Without systems engineering methodologies, the realization of complex information systems involving numerous interacting components would be prohibitively expensive, prone to failure and involve timescales unacceptable in today's defense industry. By following appropriate methodologies, highly integrated and complex Command & Control (C2) information systems can be built to interact securely on a global scale. The purpose of this research paper is to build an understanding of systems engineering processes as they apply to a large and complex information system. By the end of this paper, the reader should have an appreciation of the environment within which systems engineering occurs; understand the management skills needed to facilitate the development of complex information systems and the information assurances needed in such an environment; and have a clear appreciation of systems engineering as applied to C2 information operations.

It is the intention of the authors to present this paper along the usual systems engineering lines including some discussion of the basic concepts of system engineering, information assurance, and interoperability; life cycle support and C2 operational considerations; and automated tools that can assist with various processes along the way.

2.0 BASIC CONCEPTS OF SYSTEMS ENGINEERING, INFORMATION ASSURANCE, AND INTEROPERABILITY

2.1 Systems Engineering. Systems Engineering is defined as an interdisciplinary process that ensures that the customer's needs are satisfied throughout a system's life cycle. When a system is considered to be something manufactured, like a computer, then its system life cycle usually has seven phases: (1) requirements development, (2) concept development, (3) full-scale engineering design and development, (4) manufacturing and deployment, (5) system integration and test, (6) operation, maintenance and modification, and (7) retirement, disposal or replacement. The system life cycle is different for different industries, products and customers.[1] However, even when a system life cycle is defined within the manufacturing process, the authors still question why requirements development comes before concept development. Concept development is the high-level process of determining and understanding customer needs. Without understanding what the customer wants in the first place, it becomes very difficult to discover system requirements. With apologies to Chapman, Bahill, Wymore, Kerzner, Shishko and other developers of the systems engineering process, there still remains a good argument as to why concept development should come first. Some authors refer to phase 2 as preliminary design rather than concept development. Perhaps this terminology is a better description of what actually happens at this stage of system development, while the task of 'concept' development is more closely aligned with phase 1.

The systems engineering process includes, but is not limited to: understanding customer needs, stating the problem, discovering system requirements, defining performance and cost measures, prescribing tests, validating requirements, conducting design reviews, exploring alternative concepts, sensitivity analyses, functional decomposition, system modeling, system design, designing and managing interfaces, system integration, total system test, configuration management, risk management, reliability analysis, total quality management, project management, and documentation. Very briefly, each of these processes are explained as follows:

- **Understanding customer needs.** The customer may or may not be fully aware of the details of what they need nor what, in the way of technology, is available. In either case, talking to your customer and gleaning the customer's needs is by far the most important first step in systems engineering.

- **Stating the problem.** This is another important task because one does not want solutions in search of a problem. Rather, systems engineering will optimize the customer's needs by stating their problem and then creating a set of alternative designs that satisfy performance and cost criteria to varying degrees. There will be trade-offs since none of the feasible alternatives is likely to optimize all the criteria[2].

- **Discovering system requirements.** There are two types of system requirements: mandatory (using terms such as *shall* and *will*) and preferred (using terms such as *should* or *want*). Mandatory requirements insure that the system satisfies the customer's operational need. These mandatory requirements typical rest on legal issues, such as not violating federal laws, or budgetary requirements. Mandatory requirements are not subject to trade-offs.

[1] Chapman, Bahill and Wymore (1992); Wymore (1993); Kerzner (1995); Shishko (1995).
[2] Szidarovszky, Gershon and Duckstein, 1986

- **Optimizing design.** After understanding the mandatory requirements, the preferred requirements are evaluated to determine the most optimum design. The preferred requirements should use scoring functions to evaluate the figures of merit[3], and should be evaluated with a multi-criteria decision aiding technique[4], because none of the feasible alternatives is likely to optimize all the criteria and, thus, there will be trade-offs between these requirements. The words optimize, maximize and minimize should not be used in stating requirements[5]. Quality Function Deployment (QFD) can help identify system requirements[6].

- **Defining performance and cost measures.** A technical performance measurement, often called a performance figure of merit, describes the result of a test. Such measurements are made throughout the evolution of the system.

- **Prescribing tests.** Early in the system life cycle the upcoming tests should be described in detail so as to prove compliance of the final system with its requirements.

- **Validating requirements.** Validating requirements means ensuring that the requirements are consistent and that a real-world solution can be built and tested to prove that it satisfies the requirements.

- **Conducting design reviews.** After the system model has been simulated and validated the requirements are reanalyzed and reformulated. This is called a preliminary design review.

- **Exploring alternative concepts.** Alternative designs should be proposed. Multi-criteria decision aiding techniques should be used to reveal the *best* alternatives based on performance and cost figures of merit. For the design of any complex system, alternative designs reduce project risk.

- **Sensitivity analyses.** Sensitivity analyses can be used to point out the requirements and parameters that have the biggest effects on cost, schedule and performance. They are used to help allocate resources[7].

- **What-If analysis.** Closely akin to sensitivity analysis, what-if analyses allow designers to try specific trade-off options by changing parametric values to determine the overall impact upon the resultant system. Many respected engineers consider sensitivity and what-if analyses to be one and the same thing, and the terms are often used interchangeably. Although these may, in fact, represent two sides of the same coin, the authors find the concepts and uses distinct and unique.

- **Functional decomposition.** Systems engineers do functional decomposition on new systems (1) to map functions to physical components, thereby ensuring that each function has an acknowledged owner, (2) to map functions to system requirements, and (3) to ensure that all necessary tasks are listed and that no unnecessary tasks are requested. This list becomes the basis for the work breakdown structure. Recently object-oriented analysis has been replacing

[3] Chapman, Bahill and Wymore, 1992
[4] Szidarovszky, Gershon and Duckstein, 1986
[5] Grady, 1993
[6] Bahill and Chapman, 1993; Bicknell and Bicknell, 1994
[7] Karnavas, Sanchez and Bahill, 1993

function decomposition for re-engineering existing systems[8]. Although a newer and, in some cases, more robust concept, object-oriented techniques are still in their infancy, relatively speaking, and are not suitable for every situation. The fact remains that the mapping of functional requirements and physical components must be done. The best approach depends upon a number of factors, not the least of which is the experience and hence, the 'comfort level' of the practitioners.

- **System modeling.** Many types of system models can be used, such as physical devices, equations, block diagrams, flow diagrams, object models, and computer simulations. Models are developed for alternative concepts.

- **System design.** It is called System Design for new systems and Systems Analysis for existing systems. The overall system must be broken down into subsystems, and subsystems are then decomposed into assemblies, etc. Once in its simplest form, systems engineering can then look at life cycle issues of reusability, purchasing Commercial-Off-The-Shelf (COTS) parts, etc.

- **Designing and managing interfaces.** Interfaces between subsystems, and interfaces between the main system and the external world must be designed. Subsystems should be defined to minimize the amount of information to be exchanged between the subsystems.

- **System integration.** System integration is bringing subsystems together to produce the desired result and ensure that the subsystems will interact to satisfy the customer's needs. This is where courses, manuals and training are needed[9].

- **Total system test.** The system that is finally built must be tested to see if it is acceptable to the customer and how well it satisfies the preferred requirements.

- **Configuration management.** Configuration management ensures that any changes in requirements, design or implementation are controlled, carefully identified, and accurately recorded.

- **Risk management.** There is always the risk of project failure (due to cost overruns, time overruns or failure to meet performance specifications) and risk of harm to people. Project risk can be reduced by supervising quality and timely delivery of purchased items[10].

- **Reliability analysis.** Major failure modes must be analyzed for probability of occurrence and severity of occurrence[11].

- **Total quality management.** Everyone must continually look for ways to improve the quality of the system. Major tools used in this process include basic concurrent engineering, Quality Function Deployment (QFD) and Taguchi's quality engineering techniques[12].

[8] Jacobson, Ericsson and Jacobson, 1995
[9] Grady, 1994.
[10] Kerzner, 1995.
[11] Kapur and Lamberson, 1977; O'Connor, 1991.
[12] Bicknell and Bicknell, 1994.

- **Project management.** Project management is the planning, organizing, directing, and controlling resources to meet specific goals and objectives within time and cost constraints and at the desired performance level[13].

- **Documentation.** All of these Systems Engineering activities must be documented in a common repository, often called the Engineering Notebook. Results of trade-off analyses should be included. The reasons for making critical decisions should be stated[14]. In this age of automation, this concept can and should be taken one step further. The concept of Engineering Notebooks and written reports are important and required by many customers. Still, we should be able to capture much of the engineering data, trade-offs and other rationale in some form of data structure using off-the-shelf tools. In this way, the things that we learn along the way can be made more available for search, retrieval and analysis.

2.2 Information Assurance. Our armed forces increasingly rely upon critical digital electronic information capabilities to store, process and move essential data in planning, directing, coordinating and executing operations. Powerful and sophisticated threats can exploit security weaknesses in many of these systems. Weaknesses that can be exploited become vulnerabilities that can jeopardize the most sensitive components of information capabilities. However, we can employ deep, layered defenses to reduce vulnerabilities and deter, defeat and recover from a wide range of threats. From an Information Assurance perspective, the capabilities that we must defend can be viewed broadly in terms of four major elements: local computing environments, their boundaries, networks that link them together and their supporting infrastructure.[15]

Within this paper, the term ``information assurance" is used to mean information integrity, the level of confidence that can be placed on the information, and service availability. The term information assurance applies to the collection, storage, transmission and use of information. The ultimate goal of information assurance is to protect users, business units, and enterprises from the negative effects of corruption of information or denial of services. For example, if the financial data in a payroll database is valid in the sense that it could be correct, but is not in fact correct, there may be no negative impact on the information system, but the enterprise may suffer when people get the wrong amount of money in their paychecks. Similarly, if an order for an engine part in a supply and logistics system is lost in the part of the system that dictates which pallets get loaded onto which boat, the information system continues to operate, but the supply service is denied to the person requiring the parts. Naturally, if the information systems processing, storing, or communicating information become corrupt or unavailable, that may also affect the enterprise as a whole, but simply protecting the systems without protecting the information, processing, and communication is not adequate.[16]

As the nation's information systems are being tied together, the points of entry and exposures increase, and thus risks increase. The technological advancement toward higher bandwidth communications and advanced switching systems has reduced the number of communications lines and further centralized the switching functions. Survey data indicates that the increased risk from these changes is not widely recognized.[17] Efforts made by the Defense Information Systems Agency (DISA) to promulgate standards for the Defense Information Infrastructure (DII) and the Global Information Grid (GiG) are just two examples that should have a positive impact on information assurance that will extend beyond the Department of Defense (DoD) and impact all segments of the national economy.

---

[13] Kerzner, 1995.
[14] Chapman, Bahill and Wymore, 1992; Wymore, 1993.
[15] Woodward, 2000.
[16] Management Analytics, 1995.
[17] Loch, 1992; Thyfault, 1992.

2.3 Interoperability.[18] The ability to generate and move information has increased many thousands of times over the past 30 years. The services have all become much more reliant on information technology. Unfortunately, the current capability to generate information far exceeds our ability to control and use it effectively. To ensure information interoperability, system developers must comply with data and interface standards. Understandable descriptions of databases and the data that they store are the keys to data interoperability[19]. The Information Technology Standards Guidance (ITSG) along with the Technical Architecture for Information Management (TAFIM) and its replacement, the Joint Technical Architecture (JTA), attempt to add structure to the process.

In addition there is a requirement to develop data metrics to assess and support system data interoperability. Studies done by the Center for Naval Analysis (CNA) and the C^{4}ISR Core Architecture Data Model (CADM) provide a foundation for addressing the tactical information architecture.

In a paper presented at the 1997 DoD Database Colloquium, James Mathwich made the case that the seamless flow of information is one of the most ambitious visions of information warfare. "And yet within the Department of Defense, database integration and information interoperability efforts are more often characterized as false-starts rather than successes. … Commercial data warehouse programs, which are highly bounded database integration efforts, are doing no better with no more than a 50 percent success rate. … Managing information in an interoperable community will fail unless it is automated to the greatest degree possible. Automation of information management cannot be done on a community-wide basis unless there exists a community-wide policy with sufficient detail so that it can be predictably executed in an automated tool. Integrated databases bring new information interoperability challenges. The definition and management of the linkage between information and mission has in the past been lacking. Establishing this linkage will provide critical context and metrics for managing database integration and building effective interoperable systems."[20]

From a briefing given to the Department of the Navy (DoN) Chief Information Officer (CIO) in February 1999, it is obvious that we are still concerned with interoperability issues. "Data efforts are uncoordinated and there is no process in being to fix the problem. Many C^{4}I systems are incapable of sharing and exchanging data, an interoperability problem that could result in the possible 'loss of life, equipment or supplies'. To correct the problem requires both an information architecture and a repository of systems' databases."[21]

The Joint Interoperability Test Command (JITC) performs the joint interoperability test and certification mission as prescribed in CJCSI 6212.01A[22]. From JITC we have this definition of interoperability:

- Interoperability – "The ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces, and to use the services so exchanged to enable them to operate effectively together."

[18] The Interoperability section comes from the authors' paper "Architecture: The Road to Interoperability" presented at the 1999 Command & Control Research & Technology Symposium at the Naval War College in Newport, RI.
[19] ITSG, 1998.
[20] Mathwick, 1997.
[21] Michaels, 1999.
[22] JITC, 1998.

In review, information systems and the security measures that they embody must be interoperable. They must co-exist in the same environment and not conflict with each other. They cannot impose unacceptable computing, communications or organizational burdens or obstacles that hamper accomplishment of vital operations. They should work together in such functions as sharing data and providing cues, indications or triggers to perform actions.[23]

> Winning is not a "sometimes" thing. It's an "all the time" thing. – *Vince Lombardi*

3.0 LIFE CYCLE SUPPORT AND C2 OPERATIONAL CONSIDERATIONS

The purpose of this section is to acknowledge that the development and implementation of an Information Assurance Life Cycle methodology can be the most demonstrable indicator of support toward an aggressive, proactive approach to secure information and critical information infrastructures. By incorporating "best practices" from military, industry and global government initiatives, the Information Assurance Life Cycle methodology becomes a complete solution within a Command & Control (C2) environment. A comprehensive life cycle strategy should accommodate a full range of information systems security needs – assessment, protection (implementation), validation, training, and monitoring and management. The authors believe that a life cycle, service-oriented approach that is supported by the best security technologies available is the proper approach to protecting critical C2 information and infrastructures.

The fundamental principle of the Information Assurance Life Cycle methodology requires that security measures must be implemented with the intent of providing long-term, continuous protection. The logic is simple: even if a C2's infrastructure is secure today, it may not be tomorrow. New risks and vulnerabilities are introduced at an alarming rate and new technologies are being developed and implemented just as fast. New hardware and software platforms are constantly being installed; new features, functions, and capabilities are being created, etc. More ominously, the skill, sophistication, and motivation of system hackers seem to be increasing proportionally. The critical challenge, then, is to keep IT configurations current and to do it on a continuing basis.

The Information Assurance Life Cycle is a framework best represented by a series of five basic operational phases that protect critical C2 assets. The protection is accomplished by establishing a defensive perimeter around them. Each phase is a precursor to or continuation of every other phase in the life cycle, forming a secure barrier that offers uninterrupted protection as systems grow and evolve.

At the core of this protective perimeter is the security architecture, surrounded closely by security policies and procedures and any other security measures that make up an actual security posture. Therein lies the critical data that the Information Assurance staff becomes responsible for protecting.

In 1998 the General Accounting Office (GAO) reviewed whether DoD organizations were complying with interoperability testing and certification requirements for Command, Control, Communications, Computers, And Intelligence (C^4I) systems; and what actions, if any, were needed to improve the current certification process.[24] The GAO review was not promising. Of the 15 fundamental weaknesses noted by the GAO, the Command & Control area is the most fitting for this paper:

> *COMMAND & CONTROL: DoD does not have an effective process for certifying existing, newly developed, and modified C^4I systems for interoperability; many C^4I*

[23] Woodward, 2000.
[24] General Accounting Office, 1998.

systems have not been certified for interoperability and, in fact, DoD does not know how many require certification; and improvements to the certification process are needed to provide DoD better assurance that C4I systems critical to effective joint operations are tested and certified for interoperability.

Perhaps an Information Assurance Life Cycle Methodology would be the foundation for such an effective process?

3.1 The Information Assurance Life Cycle Methodology.[25] The authors propose a simple 5-phase life cycle approach to information assurance: assess, protect, validate, train and monitor/manage.

3.1.1 Phase 1: Assess. Assessing a C2 organization's current security posture is generally the first step to resolving the myriad complex information assurance issues facing it today. The question, put bluntly, is not whether information system resources and critical assets will be compromised but when. Far too many organizations have little notion of the risks their information infrastructures face, the value of the information systems themselves, or the value of their intellectual capital and classified or "sensitive but unclassified" data. Most organizations confront these issues only when sifting through the debris left behind following a disastrous breach in what was supposed to be a secure system, or following the misappropriation of critical assets.

Information Assurance Assessment establishes the baseline that is the current state of information assurance within an organization. Using this baseline as a starting point, the Information Assurance staff can help its organization develop strategic and tactical security objectives that evolve along with the organization. The assessment process evaluates the security of an organization (both physical and logical), identifies assets to be protected, identifies security vulnerabilities, and then recommends protective options for eliminating or mitigating security risks.

The complex information assurance issues in open networks (e.g., the Internet) and Wide Area Networks (WANs), as well as on closed defense networks, is a reality in today's IT environment. Under such conditions, the Information Assurance staff becomes responsible for meeting the information assurance needs in command, control and communications, protecting intellectual property, safeguarding financial transactions, and having reliable and secure activity.

The optimal life cycle strategy begins with an assessment from multiple perspectives, ranging from physical security, to the configuration of the firewalls, to the reliability of personnel. Information Assurance remains cohesive throughout the life cycle. It takes a system perspective to ensure that any new partial solutions remain compatible with the remainder of the system. Clients, servers, databases, infrastructure protocols and links, router and firewall configurations, policies, and procedures all have their individual issues, as well as an impact on the overall level of trust placed on Information Assurance.

Assessing the risks inherent in each must be done in the context of the Information Assurance policy and objectives. Topics typically covered in an assessment include:

- Physical Network Architecture
- Onsite review of operations and physical security
- Network description (functions, topology and components)
- Network services and protocols
- Audit trials logging, alarms, and intrusion detection

[25] With special thanks to Terry DiVittorio, CISSP Senior Information Assurance Engineer/Consultant, EDS Information Assurance Services.

- Firewall, clients, servers, routers, bridges
- Internal and external connections
- Information security standards, procedures, and policies
- Procedures, responsibilities, tasks, and authorizations
- Management Network Infrastructure
- Management access
- Management functions (e.g., change, problem, security)

3.1.2 Phase 2: Protect. Command and Control organizations must clearly demonstrate their efforts to protect their information systems environment from a breakdown in accountability, privacy, confidentiality, availability, and data integrity.

Preventing unauthorized access to information assets, protecting against intentional or accidental damage – especially as the use of information technology grows among non-technical users – creating systems that are easy to use, and maintaining a protective shield around those systems requires a sure, methodical approach that addresses forward-thinking strategies as well as current goals. Information Assurance Protection provides enhanced levels of total system security by implementing advanced security technologies using field-proven secure system engineering methodologies. Public Key Infrastructure (PKI) technologies identify and authenticate users over the Internet, intranets, or extranets. Privacy and data integrity are achieved using encryption technologies and hashing algorithms. Digital signatures (now as binding in court as inked ones) provide the basis for non-repudiation. Access control allows only trusted users to view confidential data. Smart Cards, tokens, and biometrics facilitate the positive identification of users so they can be quickly and automatically routed to the information they require.

The principle task accomplished during this phase of the life cycle is the implementation of solid architectures, plans, and policies for integrating robust security practices enterprise-wide that ensure maximum levels of security and productivity.

3.1.3 Phase 3: Validate. The third phase in securing a C2 organization's information systems and infrastructure is to validate that the security mechanisms put in place during the protection phase do indeed adequately address security policy and address the risks and vulnerabilities identified during the assessment phase. How? By comparing the results of the protection phase against (1) the original requirements, (2) additional exposures, (3) vulnerabilities identified in the assessment phase, and any intervening changes in requirements and/or the IT environment.

Validation should always be done following the implementation of any new protective measure, whether the measure is as simple as the installation of a new firewall or as complicated as developing and testing a command security policy. Indeed, continual re-verification of a command's security posture is one of the requirements for re-accreditation if the systems need government security level certifications.

Information Assurance Validation consists of a set of standardized capabilities and processes that help determine the suitability of a system for a given operational environment. These capabilities help reduce fraud, mission failures, and embarrassing information and data leaks while increasing overall information system assurance. The defined processes provide standardization for the acquisition, operation, and sustainability of IT systems that collect, store, transmit, or process information.

It is essential for commands to look at information systems validations as a basic necessity – a tool for ensuring confidence in the data from which decisions are made. Information Assurance Validation provides commands with a high degree of certainty that the IT systems will operate within an

acceptable risk environment. As appropriate, the information systems infrastructure is periodically re-tested to determine how well products, applications, policies, and procedures are functioning in accordance with a given standard – defined from government-wide to local command levels – and reassessed to determine the impact of any new threats.

These validations target existing technologies, as well as emerging ones. System, plan, and procedure reviews are conducted to verify that all components are operating within established parameters and that contingencies are addressed and newly implemented technologies are appropriately configured.

3.1.4 Phase 4: Train. Information Assurance Training, the fourth phase in this life cycle model, ensures that organizational support personnel are appropriately trained and skilled in all Information Assurance service areas. In short, that they have acquired the precise technical expertise necessary for an organization's protective security measures to achieve optimum results. The training phase also provides more generalized security awareness training for staff and management to help them understand the importance of maintaining a rigorous defensive perimeter. Industry-recognized certifications are offered through a variety of Information Assurance programs. The following are just a few of the more well known:

- **Certified Information Systems Security Professional (CISSP).** This certification is from the International Information Systems Security Certification Consortium, or ISC^2 (www.isc2.org).

- **Certified Protection Professional (CPP).** The American Society for Industrial Security (www.asisonline.org) administers the Certified Protection Professional program.

- **Certified Information Systems Auditor (CISA).** With more than 23,000 members in over 100 countries, the Information Systems Audit and Control Association (www.isaca.org) is a recognized global leader in IT governance, control and assurance.

- **Business Continuity Professional Certifications.** DRI International's (DRII) world-renowned professional certification program acknowledges an individual's effort to achieve a professional level of competence in the industry. The program includes:

  - **Certified Business Continuity Professional (CBCP).**
  - **Associate Business Continuity Planner (ABCP).**
  - **Master Business Continuity Professional (MBCP).**

In addition to the organizations listed above, many accredited colleges and universities have developed certification and/or degree bearing programs in the fields of Information Assurance and Information Security.

3.1.5 Phase 5: Monitor/Manage. The fifth phase in the Information Assurance Life Cycle addresses the need for constant, active vigilance at the defensive perimeter, including security policies, practices, procedures, and processes, as well as disaster recovery and business continuity plans.

The broad adoption of the new communications media, new ways of doing business, and the Internet presents Command & Control organizations with some thorny challenges. Virtually everyone in the global command & control structure is heavily influenced by the possibilities of worldwide distribution and dissemination of information. C2 organizations that process high-volume / highly-secure

requirements and also rely on an Internet presence are faced with the very real possibility of lost or compromised information if they cannot ensure the availability, performance, privacy, confidentiality, and integrity of their new globally visible Web-based infrastructures and applications.

Information Assurance Monitoring & Management Services facilitates continued, secure electronic utilization over the Internet, intranets, extranets, and virtual private networks. It provides a layered, defense-in-depth strategy to adequately secure, monitor, protect, and manage a C2 organization's critical information environment, including intrusion detection and response. The capabilities within this service assist in controlling the major security threats faced by today's digital enterprises, providing proactive as well as reactive network operations center services 24 hours a day, 365 days per year.

3.1.6 Life Cycle Summary. Cycling just once through the five-step life cycle model, though, isn't enough. Change is happening at a rapid rate – in any organization, in technology, in the economy. And with each new change comes a new set of security challenges that must be assessed, protected against, validated, trained for, and monitored. The life cycle approach must be rigorous, repeatable, and measurable. The Information Assurance staff must be able to get the continual assurance they need that their applications, systems, and critical data are secure when accessed or deployed any time, anywhere.

The Information Assurance staff may also be responsible for building security into IT solutions based on a System Life Cycle methodology that integrates security requirements into each phase of the systems development life cycle. Integrating security into the development and maintenance of secure applications is more than just another good security strategy. It becomes an imperative. Integrated security mechanisms result in a higher level of cost-effective security. One must realize that the right amount of security must be integrated into a command’s applications from the outset. This further reduces costs typically associated with "grafting" security features onto existing systems after the fact.

Unlike many niche solutions, a rigorous, repeatable, and measurable process such as an Information Assurance Life Cycle methodology would be standardized and far-reaching, embracing a wide variety of security products, systems, and mechanisms. A comprehensive life cycle information assurance solution must be based on proven processes.

While the opportunities and rewards are great, potential security hazards lurk at every juncture, every interface, and every portal. Establishing and maintaining effective policies that address the security, integrity, availability, confidentiality, and privacy of critical information system assets is crucial to the survival of a C2 organization.

Specifically, C2 organizations must put into operation and institutionalize a set of security measures (hardware, software and data), along with their controlling policies, practices, and procedures. These must address the full range of exposures, vulnerabilities, threats, and risks created by the new model. To that end, a truly robust set of security services, implemented in accordance with an Information Assurance life cycle methodology, is the surest way to mitigate risk now and in the future.

An effective life cycle methodology will provide the full range of security services required to protect the C2 organization on an ongoing basis:

- Security assessments to assess the C2 organization's current security posture and recommend the appropriate security policies, processes, and procedures.
- Development and implementation of protective measures, including security policies, plans, and architectures that address the identified exposures.
- Validation of the C2 organization's information systems infrastructure, following the implementation of security measures.

- Personnel training to ensure the continued security of the C2 organization's information systems.
- Procedures to continuously monitor the security status of systems and to manage and administer the C2 organization's security policies, processes, procedures, and security technologies.

The Information Assurance Life Cycle methodology delivers the skills, tools, and resources needed to keep data secure and to protect physical, financial and intellectual capital from assault and compromise. End-to-end, the life cycle methodology helps C2 organizations gain control over user access, simplify security management and administration processes, improve accountability and data integrity, ensure privacy and confidentiality, and guard against costly security breaches . . . across platforms, over the Internet, and around the world.

4.0 AUTOMATED TOOLS

Anyone operating an Information Assurance Program will learn to recognize the value and limitations of automated information assurance tools. There is an entire range of tools that can assist in managing an information assurance program, including: attribute tools; information handling tools such as database management systems and data visualization tools; architecture tools; interoperability tools; risk, threat and vulnerability assessment tools; requirements tools; network security auditing and anti-virus tools; policy and process tools; graphical interface tools; simulation and modeling tools; and even the tools that attackers use to attempt to access and compromise your automated information. This section will briefly mention a few so that the reader can get an idea of what is available.[26]

- **Information Handling Tools** include database management systems like MS Access® and Oracle®, or data visualization tools such as Starlight® by Battelle.

- **Architecture Tools** range from simple databases to sophisticated analysis models. Examples include Data Analysis and Visualization Environment (DAVE)® by Donnell Associates, Inc. (DAI) and Architect, a Navy specific implementation of DAVE.

- **Interoperability Tools** come in lots of flavors. Some simply catalog functionality; some, like Levels of Information System Interoperability (LISI)® by Mitre Corporation provide a subjective assessment of interoperability issues; and some actually assist the Certification and Accreditation (C&A) process. The Secure Interoperability Testing Database currently under development by the Joint Interoperability Test Command (JITC) is a good example of the latter.

- **Risk, Threat and Vulnerability Assessment Tools,** like interoperability tools are ubiquitous. Some are designed specifically for physical security modeling, some for the "Cyber" or information venue, and some are more generic. Examples include RiskWatch® by RiskWatch, Inc., and the Common Criteria Toolbox®, originally developed by Sparta under the sponsorship of the National Information Assurance Partnership (NIAP) and the international Common Criteria community.

- **Requirements Tools** range from simple database implementations like the Defense Information Assurance Agency's (DISA) Requirements Tractability Matrix (RTM), the

[26] Special thanks to Stephen Quinn at the National Institute of Standards and Technology.

Common Criteria Toolbox® mentioned above, and Computer Aided Systems Engineering (CASE) tools like Teamwork®, TAGS® and others too numerous to mention.

- **Internal Vulnerability Scanning/Auditing Tools** would include things like the Computer Oracle and Password System (COPS)® package from Purdue University, and Cisco's Net Ranger®.

- **Password Enhancing Tools/Authentication and System Security Tools** are often built into operating systems and application packages but there are also add-on programs that provide additional services and enhanced security such as OPIE® (One Time Passwords in Everything) developed at the US Naval Research Laboratory (NRL).

- **Password Breaking Tools** abound on the Internet making them readily available to anyone with an interest; e.g., Crack, Brutus, etc. Brutus was first made publicly available in October 1998 and since that time there have been at least 70,000 downloads and over 175,000 visitors to their website. Many of them, no doubt, are those who want to break the passwords on your system! The webpage states: "Development continues so new releases will be available in the near future."

- **Access Control Tools** would include tools like Kerberos®, the network authentication protocol from the Massachusetts Institute of Technology (MIT).

- **Logging Tools** like LogTime®, a small utility that performs time and cost tracking.

- **Mail Security Tools** help ensure the privacy and confidentiality of email and other documents. One of the most popular examples is Pretty Good Privacy (PGP) ® from Network Associates.

- **Anti-Virus Tools** form a large segment of the industry today. Many examples are available such as Check-Up®, Dr. Solomon's Anti-Virus Toolkit®, F-PROT®, and VIRUSCAN® but probably the most well known are McAfee VirusScan® and Norton Anti-Virus®.

- **Intrusion Detection Tools/Network Monitoring Tools** would include ASAX® (Advanced Security audit trail Analysis on unix), Net Ranger® and Tripwire®.

- **Policy/Process Tools** help develop, enforce and measure the effectiveness of organizational policies, processes and procedures. Many are text based question and answer tools designed to help assess the state of the environment and capture that information in some form of database. The Requirements Tracability Matrix (RTM)®, and the Common Criteria Toolbox® are good examples.

- **Modeling and Simulation** tools tend to be very domain dependent, specifically developed to focus on a particular problem, situation or environment. However, some generic shells do exist to help develop these domain specific models. Commercial modeling tools like Microsoft's Visio® and Rational Rose® fit this category.

- **A quick summary of other tools and utilities that may be useful include:**

  - **Logging Utilities** such as raceroute;
  - **System Status Reporting Tools** like ident;
  - **Packet Filtering Tools** such as the IP packet filter for SunOs;
  - **Firewall Tools** such as socks;
  - **Real-time Attack Response Tools** such as a dummy "su" program;
  - **Encryption Tools** like IBM's Data Encryption Standard (DES)® Package;
  - **Host Configuration Tools** similar to Op®; and
  - **Cryptographic Checksum Tools** such as Snefru®.
  - **Other miscellaneous tools** such as PC-Sentry® (a collection of programs and utilities to provide security and accountability on PC's and PC networks) and SATAN® (System Administrator Tool for Analyzing Networks), a network security analyzer that scans systems connected to the network noting the existence of known and often exploited vulnerabilities.

5.0 SUMMARY AND CONCLUSIONS

As stated in the Introduction, the purpose of this research paper was to build an understanding of the systems engineering process as it applies to a large and complex information system. Hence, we focused on life cycle management within the systems engineering methodology. Systems Engineering models, practices and methodologies are not new but, until recently, they have been applied mostly to large-scale hardware or specific software application development. But these same methods apply to any large-scale system and their application within the world of Information Assurance could yield enormous benefits.

If we have been true to our purpose, the reader should now have an appreciation of the environment within which systems engineering occurs; understand the management skills needed to facilitate the development of complex information systems and the information assurances needed in such an environment; and have a clear appreciation of systems engineering as applied to C2 information operations. Consideration of Systems Engineering concepts and their application to information architectures, interoperability and information assurance is an area deserving greater emphasis and more in-depth study.

Bibliography

1. Bahill A.T. and Chapman, W.L., *"A tutorial on quality function deployment,"* Engr Management J, 5(3):24-35, 1993.
2. Bicknell, K.D. and Bicknell, B.A., T*he Road Map to Repeatable Success: Using QFD to Implement Changes*, CRC Press, Boca Raton, 1994.
3. Chapman, W.L., Bahill, A.T. and Wymore, W., *Engineering Modeling and Design*, CRC Press, Boca Raton, 1992.
4. Curts, R., and Campbell, D. *Architecture: The Road to Interoperability*, Command & Control Research & Technology Symposium, Navy War College, Newport, RI, 1999.
5. General Accounting Office, *Joint Military Operations: Weaknesses in DOD's Process for Certifying C^4I Systems' Interoperability* (Letter Report, 03/13/98, GAO/NSIAD-98-73)
6. Grady, J.O., *System Requirements Analysis*, McGraw Hill Inc., 1993.
7. Grady, J.O., *System Integration*, CRC Press, Boca Raton, 1994.
8. Grady, J.O., *System Engineering Planning and Enterprise Identity*, CRC Press, Boca Raton, 1995.
9. Information Technology Standards, *Information Technology Standards Guidance – Information Management.* Final Draft Version 1.0. Washington, DC: Department of the Navy, 1998.
10. Jacobson, I., Ericsson, M. and Jacobson, A., *The Object Advantage: Business Process Reengineering with Object Technology*, Addison-Wesley, New York, 1995.
11. Joint Interoperability Test Command, *C^4I Interoperability–JITC Certification Process*. JITC Home Page, 21 Oct 1998.
12. Kapur, K.C. and L.R. Lamberson, *Reliability in Engineering Design*, John Wiley & Sons, New York, 1977.
13. Karnavas, W.J., Sanchez, P. and Bahill A.T., *"Sensitivity analyses of continuous and discrete systems in the time and frequency domains,"* IEEE Trans Syst Man Cybernetics**,** SMC-23: 488-501, 1993.
14. Kerzner, H., *Project Management: A Systems Approach to Planning, Scheduling, and Controlling*, Van Nostrand Reinhold, New York, 1995.
15. Loch, K. D., Houston H. Carr, and Merrill E. Warkentin, Thr*eats to Information Systems: Today's Reality, Yesterday's Understanding*, MIS Quarterly (June 1992): pp. 173-186.
16. Management Analytics, *Planning Considerations for Defensive Information Warfare – Information Assurance.* Prepared for Defense Information Systems Agency (DISA) Joint Interoperability and Engineering Organization (JIEO) Center for Information Systems Security (CISS) - December 15, 1993
17. Mathwick, James E. "*Database Integration, Practical Lessons-Learned*." San Diego, CA: DoD Database Colloquium, 1997.
18. Michaels, R. "*Department of the Navy Data Interoperability*." Briefing to Mr. Dan Porter, DoN CIO. Arlington, VA: GRC International, 18 February 1999.
19. Shishko, R. *NASA Systems Engineering Handbook*, SP-6105, 1995.
20. Szidarovszky, F., Gershon, M. and Duckstein, L., *Techniques for Multiobjective Decision Making in Systems*, CRC Press, Boca Raton, 1993.
21. Thyfault, M. E., Stephanie Stahlwith, and Joseph C. Panetteri, *Weak Links*, Information Week (August 10, 1992): pp. 26–31.
22. Woodward, J.L., Jr., LGEN, USAF, Director for Command, Control, Communications and Computer Systems, The Joint Staff, Pentagon. *Information Assurance Through Defense in Depth*, February 2000.
23. Wymore, W., *Model-Based Systems Engineering*, CRC Press, Boca Raton, 1993.

Vita

CDR Raymond J. Curts, Ph.D., (USN, Ret.) was born December 2, 1946 in Philadelphia, Pennsylvania and is an American citizen. He graduated from Vandalia Community High School, Vandalia, Illinois in 1965. He received his Bachelor of Science in Aeronautical and Astronautical Engineering from the University of Illinois in 1970 and was commissioned as an Ensign in the United States Navy. In December 1972 he earned his wings as a Naval Aviator and was assigned to the U.S. Naval Base at Guantanamo Bay, Cuba. Returning to the continental United States in 1976, he became an instructor pilot in the Navy's Advanced Jet Training Command in Beeville, Texas where he earned a Master of Arts degree in Management and Business Administration from Webster College of St. Louis, Missouri. After tours of duty in Norfolk, Virginia; Rota, Spain; and Key West, Florida, he was stationed at the Space and Naval Warfare Systems Command (SPAWAR) in Washington, DC where he spent five years as the Navy's Electronic Warfare Architect. During this time he earned a Ph.D. in Information Technology from George Mason University. Since retirement from the Naval service in 1992, Dr. Curts has supported a wide variety of government agencies with several major corporations. Currently he is providing Information Assurance and systems integration support to the National Imagery and Mapping Agency, the U.S. Navy and several other government agencies.

LCDR Douglas E. Campbell, Ph.D., (USNR-R, Ret.) was born on May 9, 1954 in Portsmouth, Virginia, and is an American citizen. He graduated from Kenitra American High School, Kenitra, Morocco, in 1972. He received his Bachelor of Science degree in Journalism from the University of Kansas in 1976 and was immediately commissioned as an Ensign in the United States Navy. He joined the U.S. Naval Reserve Program as an Intelligence Officer in 1980 and was transferred to the Retired Reserves as a Lieutenant Commander on 1 June 1999. Dr. Campbell received his Master of Science degree from the University of Southern California in Computer Systems Management in 1986 and his Doctor of Philosophy degree in Computer Security from Southwest University in New Orleans, Louisiana, in 1990. Dr. Campbell is president and CEO of Syneca Research Group, Inc., a certified 8(a) and Small & Disadvantaged Business entity under the U.S. Small Business Administration’s program. His clients include the U.S. Federal Aviation Administration, Smithsonian Institute, U.S. Navy, U.S. Department of Justice, and NASA.