Securing the Future:
Implementation of the Global Command & Control System

Joseph P. F. Herdt, Lt, USAF
Cape Canaveral Air Force Station, Florida

Introduction

"Hi, this is Lieutenant Derth, I'm the assistant systems administrator for the Cape Canaveral Air Force Station's Global Command and Control System. We're having some problems installing the client software onto the workstations and I need some advice on implementation."

"OK Lieutenant, you'll need to talk with Lieutenant Derth regarding that problem. Our office does not support that system implementation yet."

Lieutenant Derth scratched his head and let out an audible exasperated gasp. The network systems contractor on the other end of the phone just informed the good Lieutenant to consult with himself for further information and assistance regarding the implementation problems he was experiencing.

Lieutenant Derth only got involved with the systems implementation six months ago, and the process had been ongoing for at least three years now. In his mind, some of the primary implementation questions still remained unanswered. What security measures should be taken to safeguard sensitive data and information? How would the system fit into the existing information technology architecture? Who would be responsible for maintaining and supporting the system after the initial implementation? Obviously, Lieutenant Derth was in need of assistance, but where could he turn to for support?

Secure Communications

The requirement of secure communications is one of ever-increasing concern for both governmental and corporate organizations. Effective, secure distribution of data and information is essential to meet mission and business objectives (Loch, et al., 1992). Information is the lifeblood of most organizations in today's fast-paced, information-driven economy. An organization's sensitive or proprietary data and information are always in danger. As information technologies, including computers and communication systems, evolve in the current dynamic environment, the threats to this information may change; however, they will never disappear (Intelligence Threat Handbook, 2000). It is imperative that organizations develop, implement, and manage an effective, secure information distribution system, including specific policies and procedures to reduce the threat of potential loss of sensitive or critical information.

In an effort to capitalize on advances in information technology, the Department of Defense has spearheaded several projects, which strive to take advantage of current communication technologies to enhance mission operability. These projects include the Secret Internet Protocol Router Network (SIPRNET), Common Operating Environment (COE), and the Defense Messaging Service (DMS). These three projects make up the foundation of the Global Command and Control System (GCCS) (DMS Global Solutions, 1999).

It is important to note that certain aspects of the system discussed in this case study, and specific implementation information is deemed sensitive. The sensitive nature of the system therefore directs a limited discussion on several system specific details. Therefore, this study will focus on generalized principles, which are demonstrated, within constraints, by real-world system implementation issues. All information presented in this case is to be considered unclassified/non-sensitive.

Global Command and Control System

In September 1992, the Assistant Secretary of Defense established the Global Command and Control System as the principle migration path for defense-wide command and control systems (C4I[1] For The Warrior Brochure, 1999). Department of Defense (DoD) organizations, including military service branches, were given direction to migrate to the new communications system within five years, effectively replacing existing classified and sensitive communications systems (Defense Information Systems Agency, 2000). Further, effective migration was time critical, as existing outdated information distribution systems would no longer be supported. The Assistant Secretary of Defense commanded that GCCS should be developed and implemented through maximum use of commercial off-the-shelf and government off-the-shelf components. In this way GCCS could be rapidly and efficiently delivered to combatant commanders to provide command and control ($C2^2$) capabilities. Further, he specified that the program must have the capacity to evolve through a continuous requirement refinement process to meet the goal of providing responsive C2 to combatant commanders (C4I For The Warrior Brochure, 1999).

Q1: What are the advantages of utilizing off-the-shelf components versus developing in-house products?

The need for GCCS stems directly from the problem of non-uniform information systems within the DoD. The DoD information systems network con-

sists of a jumble of various information systems loosely linked together. Multiple protocols are utilized to operate the various networks. This non-uniformity in information systems gave rise to the proliferation of non-homogeneous data (Intelligence Threat Handbook, 2000). Although each system worked adequately within the particular mechanism for which it was built, there was no interoperability with other components. Yet each component had information that needed to be shared with other constituents.

For example, individuals working with imagery data had excellent applications to analyze and extract relevant information. However, there was a significant lack of functionality in the dissemination of such data. Imagery applications were not linked to interconnected networks. Therefore, by the time the necessary data was received by the users, the data was out-of-date, and often corrupted and unusable.

GCCS subjugates the problems with non-conformity by implementing standard data[3] principles via a common operating environment; thus providing a common look and feel to all user applications and interfaces. GCCS is composed of several mission applications built to a single common operating environment networked to support sharing, displaying, and passing of information and databases (C4I For The Warrior Brochure, 1999).

Q2: What are some of the possible solutions to the non-uniformity problem?

System architects stressed the requirement for developing a system that could be rapidly implemented; thereby, providing solutions for the non-uniformity problems. Developers used existing technologies, proven to interface effectively. GCCS has evolved from an initial baseline of existing C2 components, serving as the cornerstone for the rapid implementation of an initial system capable of fulfilling the most immediate user requirements (C4I For The Warrior Brochure, 1999). As new GCCS versions are subsequently fielded, additional existing legacy systems will be replaced and secured. The common functional, physical, and operational characteristics of GCCS are based on a single Common Operating Environment[4] (COE). All future Joint and Service/ CINC[5] unique mission applications must be compatible with this COE. The Department of Defense will retain a fully integrated, single GCCS, with all applications having a common look and feel. GCCS gives the warfighter a highly flexible system capable of collecting, processing, disseminating, and protecting information to support critical decision-making and to achieve unity of effort and command dominance (Noe, 2000).

Interoperability has been the driving force in implementing GCCS. Common mission applications, databases, imagery, teleconferencing and open architectures are key tenets in providing a single joint Command and Control system. The system has been designed to grow to meet the needs of the warfighter of the future and the challenges of multiple regional conflicts.

Case Study Site

The mission of the 45th Space Wing is stated as '*Enhance national strength through assured access to space for Department of Defense, civil, and commercial users.*' In accordance with this mission statement, the 45th Space Wing conducts space launch operations[6], placing satellites and other spacecraft on orbit.

The 45th Space Wing is composed of the Cape Canaveral Air Force Station (CCAFS), and Patrick Air Force Base. CCAFS contains the hardware, facilities, and personnel necessary to conduct space launch operations, while Patrick Air Force Base serves as an operational support base for CCAFS (Figure 1).

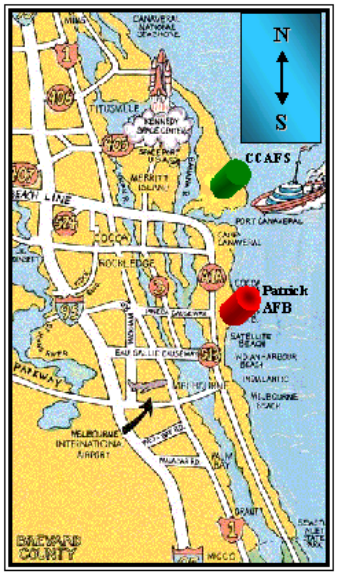

Figure 1. Map of Brevard County, Florida coastline detailing location of Patrick Air Force Base (AFB) and Cape Canaveral Air Force Station (CCAFS) (www.patrick.af.mil)

Launch operations, including Space Shuttle support, are conducted from interrelated organizations called squadrons, structured to perform specialized operations in support of differing launch systems. Squadrons, and their associated facilities are often geographically separated; therefore necessitating a complex communications infrastructure.

Implementation Background

In June 1995, the GCCS system was successfully implemented into the 45th Space Wing Command Post[7] located at Patrick Air Force Base, Florida. Although Patrick AFB, the support base for Cape Canaveral Air Force Station (CCAFS), had GCCS operability, connectivity was non-existent at CCAFS. The lack of GCCS connectivity significantly inhibited the ability to access secure information and receive valuable message traffic.

The initial requirements for the implementation of the GCCS system into CCAFS were developed and submitted to the 45th Space Wing Support Group in July 1997, almost five years after the directive to implement the system. In a letter to Headquarters US Space Command (HQAFSPC), Brigadier General F. Randall Starbuck stated the original requirements for a GCCS systems implementation at CCAFS as:

"…connect the 1st Space Launch Squadron (SLS), 3rd SLS, 45th Range Squadron, 45th Weather Squadron, 45th Operations Support Squadron, and our Maintenance and Operations Coordination Center."

With this management directive, cross-functional development and implementation teams were assembled to facilitate the implementation of the GCCS system. Team members consisted of individuals from key departments including, 45th Space Wing Communications Squadron, 45th Space Wing Security Forces Squadron, 45th Space Wing OSI, 3 SLS, 1 SLS, 5 SLS, 45th OG, 45th

RANS, 45th WS, and JBOSH Communication Systems Contractors. Numerous meetings followed over the next year defining technical requirements, installation schedules and contractual support.

In August 1998, the development teams presented a consolidated report to management. The report identified the units within the 45th Operations Group[8], and other sponsored agencies who required GCCS. The report recommended seven operational GCCS stations be implemented into the 45th Operations Group. Management reviewed the report and concurred with the recommendations, thus authorizing seven operational GCCS stations.

To further complicate design and implementation, it was determined to be expeditious to combine the upgrade of the outdated AUTODIN system to the new Defense Messaging System (DMS)[9] with the CCAFS requirement for GCCS connectivity.

Hardware and software procurement began in December 1998, and final equipment procurement was completed in October 1999. Procurement delays occurred due to equipment delivery conflicts, stemming from the Kosovo conflict.

A primary contractor was selected for installation and testing of the CCAFS GCCS system. Outsourcing allowed the development team to purchase a complete packaged system rather than individual components. The development teams lacked the necessary knowledge and experience to adequately design and build a system from the ground up. Therefore, the team defined requirements, and independent contractors submitted proposals for complete solutions. Thus, the development team purchased not only the equipment and manpower to implement the system; it also purchased the initial maintenance and assurance of effective operability.

Several concerns dominated the decision to outsource the CCAFS GCCS system. First and foremost, the concern of adequate experience within the development team arose. It was essential that the project managers, internal to the organization, fully understood the requirements and technical aspects of the system. If this experience and knowledge were lacking, no external entity could provide a system that adequately met the needs of the organization. Another concern arose from the standpoint of whether to accept the lowest cost alternative, or the option that best met system objectives. The financial elements of the system were ever present and the desire to reduce costs and remain within budget provided for heated debate. In the end, the option that best met system requirements and mission objectives was selected.

GCCS implementation actions commenced in August 1999. Installation efforts were completed in September 2000. Figure 2 depicts a generalized timeline of the CCAFS GCCS implementation.

Q3: What are the potential complications stemming from the replacement of an outdated system?

System Architecture

The GCCS system operates on the CCAFS Secret Internet Protocol Router Network (SIPRNET) local area network (LAN) commonly referred to as the CCAFS RED LAN; constructed to provide the necessary telecommunications infrastructure to effectively operate the GCCS system. The SIPRNET is an operational information layer of the Defense Information Systems Network (DISN) utilized to transport sensitive and/or classified data and information. The SIPRNET can be most easily thought of as an Internet for classified and sensitive government information.

The SIPRNET acts as a communications infrastructure. Applications and programs, such as GCCS, utilize the SIPRNET to transfer data securely and effectively via the utilization of Internet technologies and protocols to link Department of Defense and contractor computer networks. The established SIPRNET network is physically separate from the Internet; therefore, individuals with access to the Internet cannot access the SIPRNET. Access to the SIPRNET requires specific hardware and software, which ensure proper security through encryption and authorization (DMS Global Solutions, 1999).

Figure 2. Timeline of GCCS implementation into CCAFS.

The GCCS infrastructure consists of a client-server environment incorporating UNIX-based servers and client terminals as well as personal computers; operating on a local area network (LAN). The GCCS infrastructure supports a communications capability providing data transfer facilities among workstations and servers. The SIPRNET provides connectivity between GCCS sites. Remote user access is also supported via dial-in communications servers or via Telnet from remote SIPRNET nodes (Noe, 2000)

System Requirements

Functional system requirements edict seven operational stations, which compose the CCAFS GCCS network. Workstations are located at primary utilitarian locations on CCAFS, and provide functionality to personnel working in those operational facilities. Figure 3 provides a general overview of the primary facilities, which required GCCS stations.

The GCCS system is composed of high bandwidth applications. Additionally, new applications such as video teleconferencing and real-time telemetry reporting were in the process of being integrated into the GCCS software package. Therefore, a broadband infrastructure was required to support such high data flow.

Furthermore, while the initial cadre of GCCS users was relatively small at approximately 50 users, the system required expandability as the number of users was foreseen to eventually include all of the over 6000 end-users on CCAFS. This expandability thus mandated flexible solutions that provide excess capac-

ity and ease of modification. Figure 4, provided at the end of this case, presents an overview of the GCCS network at CCAFS.

Implementation Issues

Several key issues were identified during the CCAFS GCCS development and implementation process. These issues include security, integrating a complex information system into the current enterprise IT architecture, lack of adequate direct support, training, maintenance, and future enhancements. These issues will now be discussed in greater detail.

Security[10]

Security concerns were ever present during the development and implementation of the CCAFS GCCS network. The GCCS system is designed to electronically distribute classified and sensitive information and data; therefore, it is a prime target for hackers and intelligence agents, both foreign and domestic. Table 1 details some generalized security concepts the implementation team focused on during system design and configuration. A breach in the GCCS network security represents a potential threat to national security; therefore, extreme diligence was taken when designing the system.

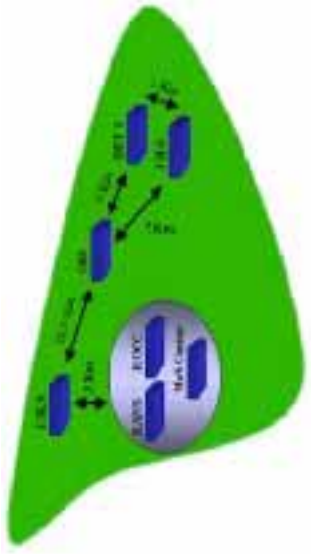

Figure 3. The primary facilities, which required GCCS stations at CCAFS. Seven GCCS stations are required on CCAFS. Stations are located in five primary facilites. Single GCCS stations are required in the 1 SLS, DET 1, 3 SLS, and OSS. The ROCC, RANS, and Mes Center are located in the same physical facility. All distances are approximated in kilometers and not to scale.

Q4: Given the general system requirements, how would you design the network?

Problem	Business Concern
Authorization	Does user have permission to access a specific computer or collection of information?
Authentication	Is the user truly who he/she purports to be?
Integrity	Did the person sending a message actually send it? Can the receiver verify that the message has not been tampered with?
Privacy	Is the communication or transaction private?
Fraud/theft	Is anyone stealing information/data?
Sabotage	Can someone enter my internal information systems and/or networks and access sensitive/ critical/private information and/ or destroy/alter information?

Table 1. The primary security problems and associated business concerns (Applegate, et al. 1999)

Security Requirements

Due to the sensitive nature of the information contained in the GCCS system, effective security at every level of the network architecture was required. Development teams ensured that the security design focused on the three main areas of security management[11]: *physical security*, *system security*, and *transmission security*. These three primary areas of security management needed to be integrated into the security architecture at every level to ensure secure distribution of information.

Physical security is concerned with controlling access to the network itself, applications on the network, and entities within the network (Defense Information Systems Agency, 2000). Physical security begins with storing the GCCS stations in facilities that allow for private, secure conversations. As per government regulations, such facilities must be COMSEC[12] and EMSEC[13] evaluated and adhere to the DoD standards for utilization of classified information.

System security is concerned with the protection of information stored on the network (Defense Information Systems Agency, 2000). System security was implemented via network configuration and establishing permissions and procedures for end-users.

Transmission security involves making sure information is secure during transmission (Defense Information Systems Agency, 2000). The problem of unauthorized access can be overcome by transmitting data in a format that is unintelligible to any intruder. Therefore, transmission of data and information is encrypted to ensure proper security.

The development team was given a relatively free hand to select hardware and software to effectively implement security. Off-the-shelf technologies were encouraged, providing they met DoD standards. GCCS security requirements did not dictate proprietary encryption devices be utilized; therefore, off-the-shelf Digital Encryption Standard (DES) certified equipment was used to facilitate implementation.

Like a chain, security is only as strong as its weakest element and therefore it is necessary to carry out risk assessment on the network as a whole. An effective procedure was developed and risk assessment is conducted routinely to identify and correct possible security shortfalls.

Q5: How would you incorporate security into the design of the CCAFS GCCS network?

Integration

It was hoped that the GCCS system could be integrated into the existing IT infrastructure. However, a vast disparity existed between the traditional CCAFS network (NIPRNET[14]) and the GCCS system architecture. The CCAFS network was well established. An effective IT architecture was in operation and a support infrastructure was already in place. In contrast, the GCCS architecture required specific hardware and software, mandated by system requirements and specifications, and little to no support architecture existed. Due to the vast disparity, plans to integrate the GCCS system into the NIPRNET were reevaluated.

The results of the reevaluation demonstrated GCCS security requirements dictated a level of operational security that far exceeded the NIPRNET. Addi-

tionally, information protection requirements provided guidance on protecting the type of sensitive and classified information stored on the GCCS network. Due to these concerns, it was decided to establish a separate physical network apart from the NIPRNET, and the CCAFS RED LAN was established to serve as the transmission conduit for the CCAFS GCCS system. To provide global connectivity, the CCAFS RED LAN was linked to the existing Department of Defense SIPRNET. Thus, the CCAFS RED LAN effectively provides the necessary telecommunications infrastructure to effectively operate the GCCS system on a global scale.

Lack of Support

A significant lack of manpower support and adequate funding during the development and implementation phases of the CCAFS GCCS system was identified. No full-time development and implementation team was assigned to this project. As with many cross-functional team projects, team members participated on a part-time basis. In other words, team members served on the development and implementation teams in addition to regular professional duties. The lack of direct support gave rise to increases in development times and costs. The initial project was slatted for full implementation by fiscal year 1997; however, funding and personnel issues produced delays in hardware and software procurement and implementation.

Training

A failure to include development of training documentation and programs during initial requirements planning led to delays in user training and utilization of the CCAFS GCCS system. The effective implementation of the GCCS system could not be accomplished without an adequate user and network manager-training program. Users required training on the system's capabilities and use prior to full implementation. Perhaps more importantly, users needed to be trained on proper procedures to ensure the security of sensitive and classified information stored on the GCCS network.

The primary cause for the lack of competent training documentation is sited as the lack of satisfactory manpower support. Training and associated documentation were not primary considerations during project initiation; therefore, resources were not allocated towards these functional areas.

Q6: Often, functional requirements and timelines take precedence over documentation and training development. Why is training so often ignored during system design and implementation?

Maintenance

The current CCAFS GCCS system lacks a proper maintenance infrastructure. Maintenance of hardware and software components has been outsourced to private vendors. However, day-to-day management functions remain in-house, but are ill defined. The complex relationship between in-house and outsourced responsibilities significantly complicates maintenance issues.

Management of the CCAFS GCCS system is the responsibility of the Network Management Office, an in-house functional organization. The Network Management Office has the task of developing and implementing policy and ensuring the network functions nominally; however, a dedicated management team is nonexistent. Various individuals loosely assigned to support the network conduct current operations. The unique requirements of the GCCS system mandate specialized training and expertise. Specific positions and personnel must be identified and trained to serve as network managers and support users.

Long-term maintenance and operational support for hardware and software of the CCAFS GCCS system was outsourced to the existing support contractor for the NIPRNET. In this way support functions were integrated into the existing support infrastructure. However, the unique infrastructure of the GCCS system often falls outside the expertise of the primary contractor. Resolutions with encryption hardware, for example, are often delayed due to lack of experience or knowledge.

Alongside lack of expertise, outsourcing has led to problems with accountability. Network managers cannot hold the contractor directly accountable. Rather, a business office with no investment or requirement for the GCCS system manages the contractor. Therefore, network managers must channel problems and misgivings through a third-party office; thereby impeding the resolution process. Such third-party management of the contractor is deemed to be ineffectual and inefficient.

Greater support must be given to the CCAFS GCCS network to ensure effective operability and maintenance. Management of the primary outsourced contractor should be the responsibility of the Network Management Office, rather than a third party organization. Insufficiencies in long-term planning and direct support, which led to delays in implementation and cost overruns, must not be allowed to continue. Additionally, support resources must be identified to develop and carry out effective network management and user training programs to ensure the correct utilization of resources; thereby gaining an effective return on investment (ROI) for IT expenditures.

Q7: The lack of qualified personnel and manpower is a significant problem in almost every system implementation. What strategies would you employ to overcome this obstacle? What specific recommendations would you make to the system designers and managers?

Q8: List some advantages and disadvantages to conducting maintenance operations via an out-sourced organization versus an in-house functional unit.

Future Enhancement

The future of CCAFS GCCS network is uncertain. It is envisioned that the network will grow to include other agencies such as the National Aeronautic and Space Administration (NASA), the US Navy, US Army and the National Reconnaissance Organization (NRO). These agencies have requirements to replace outdated information distribution systems and have expressed an interest in integrating into the existing CCAFS GCCS network. A clear enhancement

strategy is lacking at this time, including short and long-term planning. Specifications and design architectures need to be developed to incorporate future network growth.

Q9: Design a network that incorporates the necessary security and operability requirements discussed in this case study.

Q10: Write a report on the case study including the identification of the problems, the possible solutions, your costs/benefits analysis, and your recommendations.

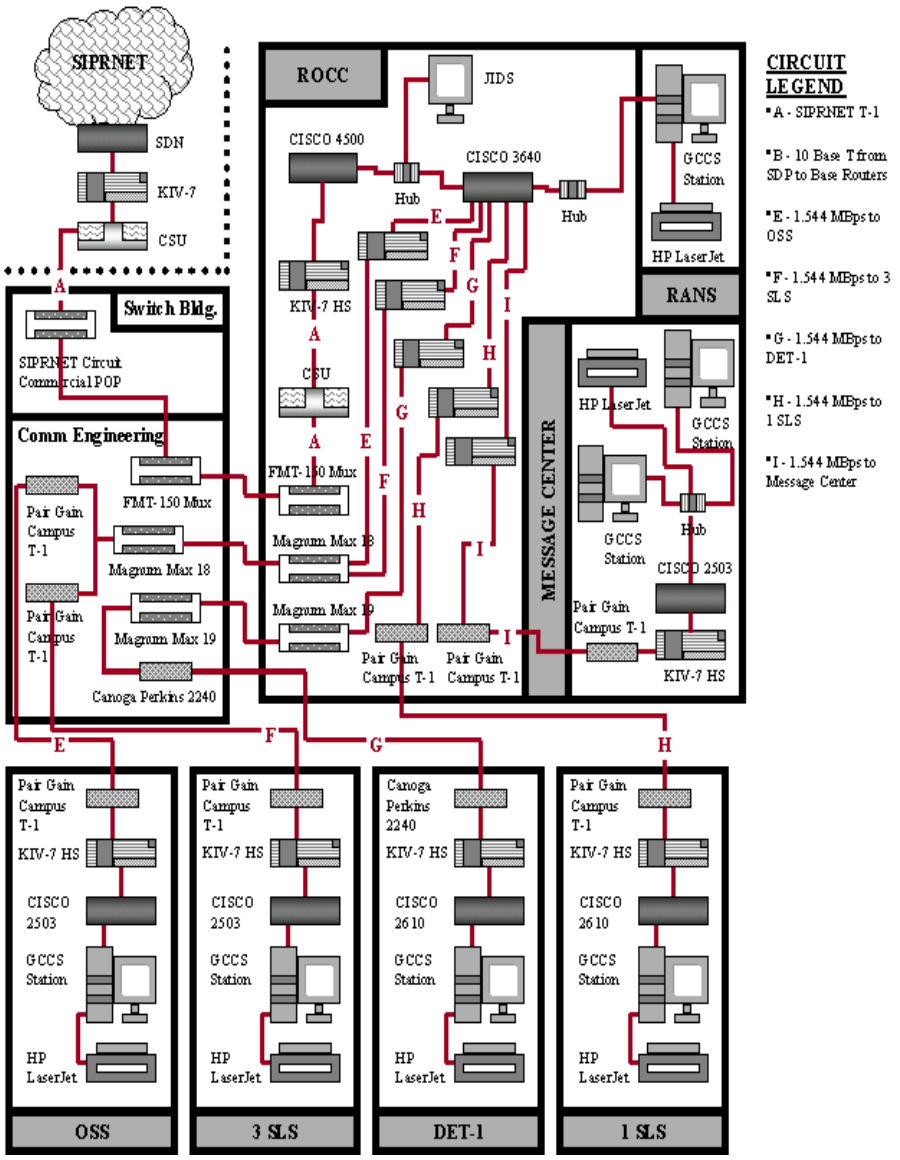

Figure 4. Schematic overview of CCAFS GCCS/SIPRNET network equipment and telecommunications infrastructure. Seven operational GCCS workstations are networked via the CCAFS SIPRNET infrastructure.

Securing the Future
Implementation of the Global Command Control System Into Cape Canaveral Air Force Station
INSTRUCTOR'S GUIDE

Synopsis

A military facility, Cape Canaveral Air Force Station (CCAFS), conducts space launch operations to place satellites and other spacecraft on orbit. CCAFS requires effective, real-time information distribution and utilizes computer-based networks to transmit and distribute sensitive and classified data and information.

Many organizations have become dependent on computer-based and telecommunications intensive information systems. Disruptions in system operability directly induce significant negative mission impacts (Loch et al., 1992). It is imperative that organizations develop, implement, and manage an effective, secure information distribution system, including specific policies and procedures to reduce the threat of potential loss of sensitive or critical information.

This case study takes place at CCAFS, Florida and depicts the development and implementation of a secure information distribution network, the Global Command and Control System (GCCS). Specifically, the case focuses on critical components of a successful integration of information distribution systems into an existing infrastructure and information technology architecture. Additionally, security requirements for secure information storage and transmission are discussed. Conclusions drawn from this study attempt to outline several key lessons learned regarding such an implementation.

Competencies

The case study was designed for a management course focusing on information technologies and project management. In order to gain a full understanding of the material presented in the case study, students should have had courses, or equivalent knowledge in:

- Systems Analysis and Design
- Computer Systems Networking
- Project Management

Teaching the Case Study

The topics and constructs discussed in the case study focus primarily on systems development and implementation. The case study is intended to provide support to a management curriculum and provide real-world insight into systems implementation and integration. Additionally, information security is a primary focus of the case study; specifically, the integration of security into the development and design of information systems.

The author recommends an integrated teaching methodology, wherein the primary concepts of systems development and implementation, and network security are covered prior to teaching the case. The case therefore serves as a real-world example to reinforce the concept taught in class. Alternatively, this case may be utilized in a seminar course to base a detailed discussion upon. The foundational concepts detailed in the case may be expounded and/or argued upon by the seminar participants.

The case could be used in a management course or a computer science course. The case study is flexible and may be modified for each instructor's needs. The class may be divided into groups to facilitate cooperative learning.

There are no simple solutions for the problems presented in the case study. Multiple alternatives exist, and students are encouraged to develop independent analyses and recommendations. Guidance regarding the primary focus of student answers is provided in this guide to facilitate the teacher in ensuring the student has addressed all core issues pertaining to this case.

Networking design tools may be helpful in the development of hypothetical systems and should be incorporated into the student analysis.

Allocated Time

Student should read the case and complete the questions prior to attending class discussion. Instructors should expect students to spend 1-2 hours preparing for the discussion.

The author recommends 1-hour of in-class discussion to effectively communicate the primary concepts in this case study. However, the case study is flexible and the time spent discussing this case may be lengthened or shortened depending upon the objectives of the instructor.

Answers To Questions

Q1: What are the advantages of utilizing off-the-shelf components versus developing in-house products?

A1: In the case of the CCAFS GCCS network, off-the-shelf components offered an effective alternative to in-house development, which was both cost-effective and time responsive. Current, proven information technologies exist, which provide secure communications. Adequate support for such off-the-shelf technologies exists, providing a reliable component at reduced costs. Additionally, the utilization of readily available components decreased the operational development and implementation time. The system development time was significantly reduced through the use of off-the-shelf technologies.

Students should stress the primary benefits of off-the-shelf technologies including:
- Reduced costs
- Readily available solutions
- Reliability and support
- Reduced development time

Q2: What are some of the possible solutions to the non-uniformity problem?

A2: The best solution to this untenable situation is the use of standard data. All data is presented in similar format and associated with the same information, whenever possible. The uses of standard data elements are key to any automated system's success, especially command and control systems. Using standard data

eliminates redundancies and provides a common foundation to facilitate information exchange.

GCCS also utilizes standardized user interfaces to facilitate use and mitigate the problems with non-conformity. The use of an effective COE allows users to easily move from one application to another. Furthermore, the use of standard data integrated into the COE allows users to view the GCCS system as a single application rather than a series of independent functional applications.

Q3: What are the potential complications stemming from the replacement of an outdated system?

A3: The potential complications are almost infinite. However, information systems only serve as force multipliers and facilitate business operations. Students should focus their answers on the loss of functionality and potential for negative impact to business operations.

In the GCCS implementation, the system developers focused their attention and the disruption to operations and the retraining of personnel in support of the new system.

The outdated AUTODIN system was omnipresent, and while it provided limited functionality, the information distributed over the system was essential to operations. It was essential to ensure that the replacement of the AUTODIN system did not negatively impact operations; therefore, a phased implementation was used.

Q4: Given the general system requirements, how would you design the network?

A4: Designing network architectures is a complex task that requires practice. There are many possible network configurations that satisfy the system requirements provided in the case. Student answers should however address the topology utilized and how the use of broadband is facilitated via the network architecture.

The GCCS network was implemented using a star topology, and possesses broadband capabilities via separate T-1 connections carrying limited traffic. Figure 4 in the case provides an overview of the network schematic. Figure 5 below demonstrates a conceptual GCCS/SIPRNET system architecture overview.

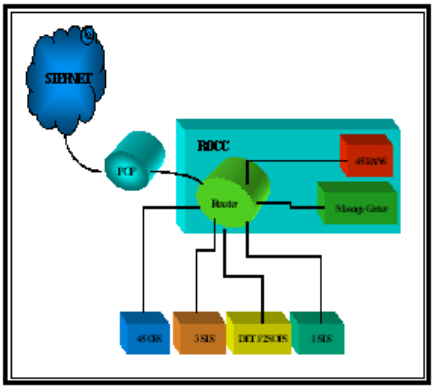

Figure 5. A conceptual schematic of the GCCS/SIPRNET network at CCAFS. Seven total stations, located at six operational sections, connected via T-1 lines compose the network. The ROCC serves as an effective network hub, which then connects to a POP and the external SIPRNET network.

Q5: How would you incorporate security into the design of the CCAFS GCCS network?

A5: Students should detail how they would integrate security into the network (Students may utilize the network designs developed in Question 4). Specifically, students should address physical security, system security, and transmission security in their answers.

Physical security is providing by storing GCCS stations in secured, isolated rooms within operational facilities with controlled access. This provides a redundant control regarding granting physical access to GCCS stations. Proper security procedures are taken to ensure access is only granted to specified individuals.

To further ensure network physical security, the CCAFS RED LAN is composed of independent telecommunications infrastructure that is physically isolated from other CCAFS networks. Alongside physical network isolation, access to GCCS terminals and applications require passwords the use of a digital encryption PCMCIA interface, encoded with a secret key.

To ensure system security, all applications and user terminals are structured with limited user privileges. Users are frequently granted read-only access and are unable to change the network and application settings. Extensive firewalls, and frequent system backups provide for protection against malicious logic and destruction of data and information. Additionally, all stations utilize securable storage equipment such as removable hard drives and backup media.

Transmission security was implemented via encryption technologies. Data and information is encrypted using KIV-7 encryption units, which are rekeyed daily to ensure proper security. Additionally, all electronic mail transmissions are encrypted via an independent system.

In conclusion, security was well integrated. A vast amount of effort was placed into designing adequate security into the system architecture in order to ensure the integrity of the sensitive information stored on the network. However, constant vigilance, defined procedures, and competent user training are required to ensure effective, secure transmission of classified and sensitive information.

Q6: Often, functional requirements and timelines take precedence over documentation and training development. Why is training so often ignored during system design and implementation?

A6: Return On Investment (ROI) can only begin once a system is in place and operational. Therefore, it is in the interest of the organization to employ new systems as quickly as possible, providing they are functionally effective. Training development is often a time consuming process that may be seen as diverting limited resources from system implementation. By foregoing effective training development, a new system may be made operational in less time.

However, while effective training development generally takes time, the lack of effective training for end-users often negatively impacts system functionality. Learning new systems take time, and errors are commonly made during the initial implementation of any new system. Effective training can mitigate such problems; thus providing a more effective implementation and help to generate an effective ROI in less time.

Q7: The lack of qualified personnel and manpower is a significant problem in almost every system implementation. What strategies would you employ to overcome this obstacle? What specific recommendations would you make to the system designers and managers?

A7: Primary strategies to overcome manpower issues involve outsourcing, training, and internal personnel acquisition. The GCCS system utilizes extensive outsourcing to conduct network maintenance and administrative operations. Additionally, training programs have been identified to which in-house personnel are to be sent. Acquisition of new personnel is not deemed possible at this time due to funding constraints.

Alongside these primary strategies, students may also want to address the allocation of resources. Currently, there remains a lack of direct support for the GCCS system. A full-time management and oversight team has yet to be assigned. System managers and network administrators strive to complete system implementation and develop operable system elements on a part-time basis. In order for the GCCS system to its reach full potential as an information distribution tool, adequate support must be allocated.

It was recommended that a full-time system administrator be assigned to manage the CCAFS GCCS network. This individual would serve to verify system requirements are met and operability is maintained; thereby, reducing possible mission impacts due to network anomalies. Furthermore, the assigned system manager will serve as a single point of contact for issues regarding the CCAFS GCCS system, such as future enhancements and adding additional resources.

Q8: List some advantages and disadvantages to conducting maintenance operations via an outsourced organization versus an in-house functional unit.

A8: In general, outsourcing maintenance operations provides internal business units to focus on primary business operations and core functions. For example, a widget sales force may outsource their network administration and thus free up resources to devote towards increasing widget sales. Additionally, outsourcing may provide for flexible solutions, as the internal organization is not required to train or acquire expertise to take advantage of new technologies. A business may migrate to a new operating system (OS) and leave the technical aspects of such a migrating to the contractor.

While outsourcing has some potential advantages, there are possible disadvantages as well. Outsourcing requires an organization to give up significant amounts of control over their networks and data; hence, flexibility may be lost. Also, a lack of internal expertise may result, leading to the organization becoming overly reliant of the contractor.

References[15]:

- Air Force Instruction 33-119, Electronic Mail (E-Mail) Management and Use, March 1999.
- Air Force Policy Directive 33-2, *Information Protection*, December 1996.
- Applegate, Lynda M., McFarlan, Warren F., McKenney, James L., Corporate Information Systems Management Text and Cases, Irwin McGraw-Hill, 1999.
- Carr, Houston H., Snyder, Charles A., The Management of Telecommunications Business Solutions to Business Problems, Irwin McGraw-Hill, 1997.
- *C4I For The Warrior Brochure*, Department of Defense, January 1999.
- *DMS Global Solutions For Secure Messaging*, Department of Defense, July 1999.
- *Intelligence Threat Handbook*. The Interagency OPSEC Support Staff, June 2000.
- Loch, Karen D., Carr, Houston H., and Warkentin, Merrill E. *Threats to Information Systems: Today's Reality, Yesterday's Understanding*. MIS Quarterly. June 1992.
- Noe, Jerry A., *Defense Messaging System Information Brief*, August 2000.
- *Operations Security: Protecting Tomorrow's Technology Today*. Defense Information Systems Agency, August 2000.
- 3d Space Launch Squadron (SLS) Operating Instruction 31-101. *Management of Executive Information Systems Management and Control*, March 2000.
- 45th Space Wing Instruction 33-108, *45th Space Wing LAN/MAN Network Policy*, August 2000.
- 45th Space Wing Instruction 91-202, *Risk Management Plan (RMP)*, August 2000.

Footnotes

1 C4I is a command strategy involving the coordination of Command, Control, Communications, and Computers functions in order to obtain and disseminate Intelligence and information. C4I attempts to facilitate the gathering and utilization of data and information via an integrated network or people, computers, and communications.

2 Command and control (C2) refers to the ability to effectively direct and monitor actions in a dynamic environment.

3 Standard data refers to the use of data wherein data elements are clearly defined, and redundant elements are excluded.

4 Defined as a standardized user interface, the COE provides a similar look and feel, as well as a common functionality, to all GCCS applications. Similar user interfaces provide a high level of usability.

5 Joint and Service/CINC operations are generalized categories of military operations. In general, Joint operations involve two or more branches of the military. Service operations are conducted by a primary branch. Air Force CINC operations are conduced by North American forces, including US and Canadian forces.

6 Space launch operations include the processing, launching, tracking, and associated project management functions necessary to launch manned and unmanned space launch vehicles.

7 The 45th Space Wing Command Post is a centralized management structure, which acts as an information focal point for operations conducted out of the 45th Space Wing.

8 The 45th Operations Group (45th OG) is the responsible government agency responsible for conducting space launch operations and testing out of the US Eastern Range.

9 The Defense Messaging Service (DMS) was developed to provide secure transfer of classified and sensitive information utilizing off-the-shelf electronic mail applications. DMS offers the flexibility and accessibility of common electronic mail applications along with the security and encryption features required to safely transmit classified data. DMS consists of all the hardware, software, procedures, standards, facilities, and personnel involved in the electronic exchange of messages between organizations and individuals in the Department of Defense (DoD).

10 Due to the sensitive nature of the GCCS system, detailed security configurations cannot be discussed in this forum; however, the general security requirements and resolutions are presented in the case and associated Instructor Guide.

11 Security management defines the procedures and protocols required to manage services such as authentication, access control, and confidentiality of information.

12 COMSEC is a governmental term for Communications Security. COMSEC ensures effective, secure distribution of data and information using secure media, and/or policies and procedures concerning the use and dissemination of information.

13 EMSEC is a governmental term for Emissions Security. EMSEC ensures that electronic emissions generated by equipment, including computers and associated infrastructure, are evaluated and controlled to ensure potential adversaries cannot elicit information regarding capabilities and/or vulnerabilities from them.

14 NIPRNET stands for Non-classified Internet Protocol Router Network. The NIPRNET is the key word for the traditional CCAFS LAN and WAN.

15 Unless deemed classified, government publications are subject to the Freedom of Information Act and therefore accessible. While specific ordering information is not available as various organizations control the specific publications used in this case-study, all non-classified publications may be obtained via a request under the Freedom of Information Act. For 45th Space Wing, and other, publications, researchers should contact the 45th Space Wing Public Affairs office at Patrick Air Force Base, Florida.

Joseph Herdt is currently the Chief, Plans & Policy and Information Operations at the 45th Operations Group, Cape Canaveral Air Force Station (CCAFS). Lt. Herdt develops operational policy and ensures effective information resource management (IRM) functionality for military space launch operations and support to commercial, NASA, and ballistic missile launches from CCAFS.

Lt. Herdt graduated from The Ohio State University with a BS in Zoology in 1997, and earned a MMIS from Auburn University in 2001. He has also received specialized military and civilian training in Network Vulnerability Analysis, Operations Security, and Information Operations.

Lt. Herdt worked as a Business Analyst and Network Administrator at Qwest Communications before joining the United States Air Force (USAF) in August 1998. After completing Officer Training School, he served as a Training Officer at Vandenberg Air Force Base, California. Stationed at the 45th Space wing at CCAFS in Florida, Lt. Herdt served as the Chief of Training for Atlas Launch Operations and subsequently the Chief, Standardization & Evaluation for Atlas Launch Operations. Following the tragic events of September 11, 2001, he assumed the new position of Chief, Plans & Policy and Information Operations. Lt. Herdt has served as a Program Manager for multi-million dollar space-launch missions and associated operation; a certified Military Training Instructor and Evaluator; and a Vulnerability Assessment Specialist and Operations Security specialist.