The Target Vulnerability Quantification Process

by

Douglas P. Vine

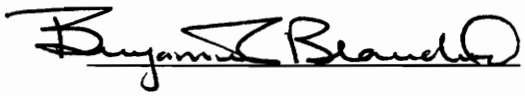
Project report submitted to the Faculty of the Virginia Polytechnic Institute and State University in partial fulfillment of the requirements for the degree of

MASTER OF SCIENCE

IN

SYSTEMS ENGINEERING

APPROVED:



Benjamin S. Blanchard, Chairman

Dr. Robert J. Beaton

Emmanuel Skamangas

September 1996

Blacksburg, Virginia

Key Words: Systems Engineering, Vulnerability Quantification, COVART

The Target Vulnerability Quantification Process

By

Douglas P. Vine

Committee Chairman: Benjamin S. Blanchard

Systems Engineering

(ABSTRACT)

The need for a target vulnerability quantification process arises from the U.S. Navy's requirement to develop defensive systems to defend civilian and military assets around the world. The systems engineering approach has been applied to improve an existing process that takes too long to perform. The functions to perform the vulnerability assessment are identified, and an automated process incorporating current off-the-shelf technologies is discussed.

The operational requirements, maintenance concept, and functional analysis are presented for the automated vulnerability quantification process. A conceptual design is then outlined for the system elements. A cost comparison between the current system and the automated system is calculated in the conceptual design.

Table of Contents

Appendix A

List of Figures

List of Tables

Introduction

Despite the demise of the Soviet Union, many countries around the globe continue their bellicose ways. Regimes in Iraq, Iran, North Korea, China, and many others continue to pose a serious threat to peace and order in various regions, or *theaters*, around the world. This threat was seen with Iraq's attempt to annex Kuwait and its subsequent launches of scud missiles at Israel and Saudi Arabia during the Gulf War. More recently, China has attempted to obstruct the democratic process in Taiwan with its show of military force in launching M-9 missiles in the Taiwan Strait.

The United States Navy is often the first force to arrive and respond in these trouble theaters. The navy must be able to defend civilian and military assets against whatever threats are launched. However, it needs to know in advance what types of threats it will be encountering. Effective defensive missile systems must be developed before these engagements occur in the theaters of operation. This is accomplished through feedback between various missile component system designers and the vulnerability analyst. As part of the vulnerability analyst's effectiveness analysis, the vulnerability of the threat targets must be identified and quantified.

Vulnerability refers to the inability of aircraft, and missiles (targets), to withstand damage or destruction when hit by enemy fire. Each of the individual components in the target has an amount of vulnerability, and each component's vulnerability contributes in some measure to the overall vulnerability of the target. The more vulnerable a target is, the more likely it will be killed when hit by the enemy threat.

The terms susceptibility and survivability are never used in the vulnerability quantification process. *Susceptibility* refers to the inability of a target to avoid being damaged in the pursuit of its mission. The degree of susceptibility is dependent on the type of mission, the lethality of the threat, and the performance capabilities and self-protection

measures of the target. The *survivability* of a target is dependent on its vulnerability and susceptibility.

The current vulnerability quantification system is made up of analysts, hardware and software. The analyst gathers intelligence data about a particular target and uses hardware and software to quantify the vulnerability of the target. In its current form, this process takes too long to perform and is cumbersome to use. It is also difficult to check errors. The goal of this paper is to develop a new system that will diminish these deficiencies while still satisfying cost constraints. This development is based on the systems engineering process outlined below.

The definition of need is described in Section 1.0. The functions that are performed in the process, and the potentially time-saving technologies being considered for the system are discussed.

Section 2.0 provides the operational requirements of the system. In order to meet these requirements, various system parameters are defined. These parameters include performance, use requirements, and measures of effectiveness. The operational life-cycle for the vulnerability quantification system is described.

A maintenance concept is developed from the operational requirements. This concept is described in Section 3.0. The maintenance concept defines the general support environment and the various levels of support required for the system. Early definition allows for the incorporation of design features that facilitate ease of maintenance. The objective of this section is to provide specific requirements that can be fully considered at later stages of the design process.

A functional analysis is performed in section 4.0. This analysis is based on the information described in the operational requirements and maintenance concept sections. It provides an abbreviated visual representation of the various steps required for operational and maintenance actions.

Section 5.0 presents the conceptual design. The goal of this section is to show how the system requirements are met. First, the system setup is defined and illustrated. Next, the allocation of system requirements to each system element is presented. Finally, a cost analysis is conducted.

Section 6.0 presents a summary of the conclusions of this paper as well as recommended future research on the target vulnerability quantification system.

1.0 Definition of Need

1.1 Current State of Target Vulnerability Quantification

The Lethality and Weapon's Effectiveness Branch (G24) at the Naval Surface Warfare Center in Dahlgren, Virginia (NSWCDD), is one of many military laboratories and civilian contractors that perform vulnerability assessments. Around the world, G24 is recognized as the authority in vulnerability quantification. This is mainly because G24 has been performing consistently accurate, detailed analyses for more than 40 years.

The amount of time to perform a vulnerability assessment at NSWCDD is directly proportional to the level of detail known about a target. Current vulnerability quantification for fighter aircraft, which are highly detailed, can take 24 to 36 months to complete. Quantifying the vulnerability of a missile target can easily take more than 12 months. The time to perform the assessment is measured from when the Naval command structure (NAVSEA and NAVAIR) hands down the target selection to when the vulnerable areas are delivered to customers. The customers include NAVSEA, NAVAIR, warhead developers, and endgame modelers (Appendix A.2). The sooner the customers can update their systems with the vulnerability quantification data, the sooner the United States can defend against these threats. Therefore, the demand for these assessments is high. If changes are not made to improve the time to perform the vulnerability quantification, other parties will continue to take over work currently performed by G24. With five analysts currently performing assessments, G24 is limited to a maximum of five missile analyses per year.

The essence of the vulnerability quantification system is the Calculation of Vulnerable Areas (COVART) software. This software has been developed specifically for G24 over the past twenty years and is currently in version 4.0. The vulnerable areas (output from COVART) constitute the product of the vulnerability assessment. Before

COVART can be executed, input files must be created and formatted. Creating and formatting input files are the functions that need to be performed to produce the product.

The process relies heavily on one vulnerability analyst, who becomes a bookkeeper of a large volume of information about a specific target. The analyst performs the assessment on a computer. However, many individual files contain a duplication of information because the process evolved from the time when assessments were performed on paper. Inconsistencies and errors can result when information is entered or updated in one file and inadvertently not updated in another file. This is an important deficiency in the current system that needs to be corrected.

One of the input files to COVART is the target computer description. Shotline Geometry (SHOTGEN) is the software tool used to plot and edit missile and aircraft geometric computer descriptions. The current software requires the vulnerability analyst to compute manually the coordinates of all the points that define components (electronics, wires, fuel, engines, structure, skin sections, and so on) relative to the nose of the target. These locations, or *facet points*, are then manually entered in a specific format in a card image file (CIMF) on the VAX operating system. The CIMF is the data file for SHOTGEN. Table 1.1 shows the data for two adjacent, solid-cylinder components. Three lines or cards are required to describe each cylinder. Typically, the CIMF contains several thousand lines of data, and the probability of data entry errors is high. Modeling errors, discussed in Section 2.2, are also high.

Table 1.1. CIMF data

X	Y	Z	Shape/Component	Card	Other Attributes					
-42.79	0.00	0.00	80058101	10	0	24	0	0	0	0 30
-45.79	0.00	0.00	80058101	20	0	24	0	0	0	0 30
7.30	9.21	0.00	80058101	30	0	24	0	0	0	0 30
-46.79	0.00	0.00	80058102	10	0	24	0	0	0	0 30
-49.79	0.00	0.00	80058102	20	0	24	0	0	0	0 30
9.21	9.21	0.00	80058102	30	0	24	0	0	0	0 30

Other input files are generated on the VAX operating system. They, like the CIMF, require the user to enter data in specific columns and rows. These files generally contain less than 1000 lines of data and the incidence of data entry errors is subsequently lower.

Errors are not easily identifiable in any of these files. A visual check can be performed to see if data lines up in the correct columns. Generally, however, the analyst must visually inspect printouts of these files; poring over each individual number. These time-consuming checks are required to ensure file accuracy.

A study of the quality of the current vulnerability quantification process in G24 appears in Appendix A. The results of the study demonstrate that the process lacks quality checks and that the computer codes are not user-friendly.

1.2 Meeting the Future

G24 is limited to a maximum of 5 missile assessments per year. However, the Navy requires an average of ten missile assessments per year. In order to complete ten assessments per year, each of the five analysts would have to complete two assessments per year. Based on other deficiencies in Section 1.1, the new process should include: user-friendly computer codes, simplified error checking, an elimination of data duplication , a reduction of hand calculations, and the data processor should be as fast as possible. Also, a constraint of $50,000 shall be placed on the acquisition , maintenance and training costs entailed in the setup of the new process.

The available technologies to realize these requirement need to be examined. It may be possible to reduce the amount of time required to perform the vulnerability quantification without sacrificing the accuracy of the assessment. The use of current off-the-shelf software can greatly assist the analysts in performing the necessary functions of computer modeling and file preparation. Any off-the-shelf software considered for use in this new system must be compatible with COVART 4.0.

Many commercial drawing packages rely on a more simplified approach to model design than SHOTGEN. In these computer-aided design (CAD) packages, a number of primitive shapes, such as cubes, cylinders, spheres, and cones, are available to the user. There are fewer points to calculate by hand, and the use of Boolean functions, such as union, intersection, and difference, on the primitives makes it easier to describe detailed components with many facet points. CAD models are produced for a variety of engineering purposes, and there are many ways to output data.

The use of database software reduces the risk of file errors, because records for each component can be created with all the relevant information required for the analysis. The necessary VAX files for input to COVART can be autoformatted from the database

software in ASCII format as reports and imported directly to the VAX working directory. If a change is made concerning the material type of a particular component, a new set of files can be created that will all contain the correct material type for it. The names of fields in a database's record remind the user of the parameter, such as the material type, that is being changed for the particular analysis. Because the computer formats the data, the likelihood of errors is reduced. Checking for errors is also simplified since all the information is located in a single, easily-readable file.

COVART is a software package that is modified several times a year to expand its usage capabilities. Therefore, to reduce the risk of different versions of COVART being used by different vulnerability analysts and to provide consistent output to G24 customers, the use of a server is preferable. In this setup, the latest compiled version of the COVART executable code resides in its own directory on the server and is accessible to all the analysts. Each vulnerability analyst accesses the server via his own personal computer and terminal emulation. A server and terminal emulation architecture could be set up easily in the G24 workspace.

An investment in new hardware may also assist in reducing the time to quantify the vulnerability of a target. Replacing the current MicroVax 2 with a new AlphaServer 200/166 MHz will improve current processing time six-fold. A forty-eight hour job can run to completion in one eight-hour work day. This time improvement is especially important when working against a deadline. Individual workstations can also improve current processing capabilities, but they are not advisable from the standpoint of cost and configuration management. The cost of an AlphaServer with 12 gigabytes of disk space is approximately $14,000, whereas the cost of a single workstation can exceed $30,000. Likewise, having many different versions of COVART on multiple machines does not ensure a consistent product.

Vulnerability analysts are aerospace and mechanical engineers. G24 currently lacks a full-time vulnerability analyst with a background in computer science. There would be many benefits to having someone in-house who understands the target vulnerability quantification process and has a knowledge of computer systems. He could provide insight into the capabilities and limitations of the software used to prepare inputs for COVART. He could assist in constructing databases, generating COVART input file formats, and troubleshooting any difficulties arising from CAD modeling. Other minor problems arising from the server and the hardware on the G24 computer network could be handled by this person. The new employee would replace one analyst from the current system and, through on-the-job training, be capable of performing a complete vulnerability assessment.

The proposed automation of the target vulnerability quantification process will reduce the time to perform a missile threat analysis from 52 weeks to 38 weeks. This will enable G24 to complete at least one more missile assessment per year.

Human errors are the result of the analyst's failure to enter data correctly or update data in the appropriate files. The frequency of this type of error is often magnified by an overwhelming amount of data to enter in a given period. The automation of the process will reduce the likelihood of human errors by reducing the amount of data entry required. Human errors are also the result of computation errors. Therefore, reducing the amount of hand computations by the analysts will reduce the number of computation errors.

1.3 Benefits

Improvements can be implemented to speed the target vulnerability process while retaining the current level of accuracy. Some of the more time-intensive tasks include generating the computer model and ensuring the accuracy of all the COVART input files.

The use of off-the-shelf CAD and database software packages offers great potential to reduce the amount of time that the human operator must spend performing hand calculations, data entry, and file checking. The time savings achieved through the purchase of new hardware will be relatively small, but the time savings near the end of the quantification process cannot be discounted when trying to meet important deadlines. The new analyst with a computer science background will ensure that the process flows smoothly. The time lost training analysts on new software and procedures must be considered, as well as the cost of acquisition and maintenance.

Reducing the amount of time to complete the assessment will reduce the amount of the cost required for the assessment. Reducing the time and cost will make G24 more competitive with the Army, Air Force, Raytheon, Motorola, and others who are vying for limited defense dollars. In the current climate of fiscal conservatism and fierce competition for government funds, it is important that G24 continue to meet the needs of the defense community effectively. This will require processing products rapidly and economically to ensure continued funding. Reducing the amount of time to complete the vulnerability quantification will also reduce the time that it takes to develop defensive missile system improvements. This will have a profound effect on diminishing the impact of weapons of terror as well as ensuring the survival of military and civilian assets around the world.

2.0 Operational Requirements

2.1 Mission Definition

The objective of the system is to provide the user with the additional tools necessary to quantify the vulnerability of enemy missiles and aircraft more rapidly than the current system while maintaining the current level of accuracy (figure 2.1). The automated system will accomplish these objectives by implementing current off-the-shelf software and hardware, by instituting quality checks and training, and by incorporating a full-time vulnerability analyst with a computer science background in the process. This system is intended for use by G24 at NSWCDD in Dahlgren, Virginia.

2.2 Typical Mission Scenario

The vulnerability analyst obtains all the available intelligence documents for the target missile. The documents contain drawings, photographs, and other relevant missile system details and are available at NSWCDD. This library of intelligence information is maintained by all organizational groups at NSWCDD through departmental overhead costs. Therefore, information is paid for each year whether or not G24 chooses to use it. Sometimes additional information becomes available during the vulnerability quantification process, and completed phases must be updated with the latest information.

Next, the computer model is generated from drawings in the intelligence reports on a personal computer with CAD software. The level of detail in the latest drawings is reflected in what is known about a particular threat missile. Often the analyst must employ his best guess as to how a particular missile system should be modeled, based on

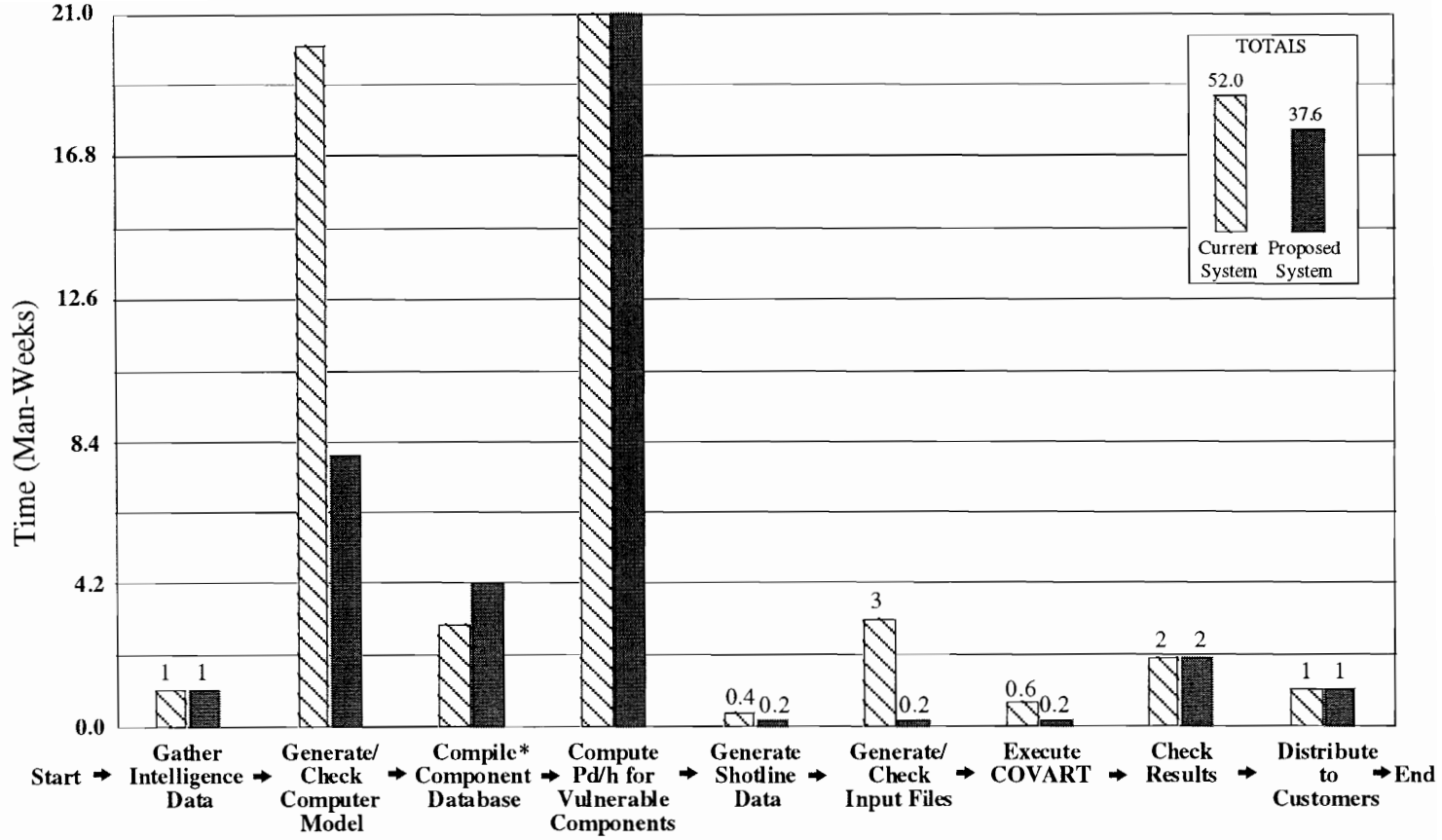


Figure 2.1. Typical Mission Profile

Notes

* New task for proposed system. The current system identifies vulnerable components and system failures only at this phase.

4.2 Man-Weeks = 1 Man-Month

precedents set by the same missile designers. Typical missile models contain three to four hundred components. These components do not need to be modeled exactly; however, size, material type, and skin thicknesses are very important. A large portion of time spent in creating a usable model goes into ensuring that the model is error-free. Model errors include overlapping components, wires, hydraulic and pneumatic lines connected to the wrong components, and components protruding from the missile skin.

At the same time as the computer model is being developed, the component database is compiled on a personal computer using database software (figure 2.2). A record is completed for each component in the model. Three to four hundred records are completed per missile model; however, only forty to sixty of the components are vulnerable. Therefore, most records do not require that all fields are completed.

The analyst then begins the time-consuming task of computing the probability of damage given a hit (Pd/h) curves for the vulnerable components. Curves are calculated based on historical test data and penetration equations embedded in the FATEPEN computer code. The penetration equations incorporate the physics of metal fragments impacting a variety of materials commonly found in missiles and aircraft. Different criteria, such as energy, momentum, and hole sizes, are used to determine what masses and velocities are required to create a specific level of damage. FATEPEN is run from a DOS prompt on a personal computer.

Next, the analyst uses VersaTerm Pro terminal emulation software on his personal computer to log onto an AlphaServer. The formatted computer description of the missile model is imported from a personal computer to a working directory on the server. A one-inch grid is placed over the geometric computer model, and shotlines are generated for twenty-six different missile aspects by varying the azimuth and elevation using the FASTGEN code that resides on the server. Shotlines are rays that intersect normal to the grid. They represent the path of fragments traveling through the target.

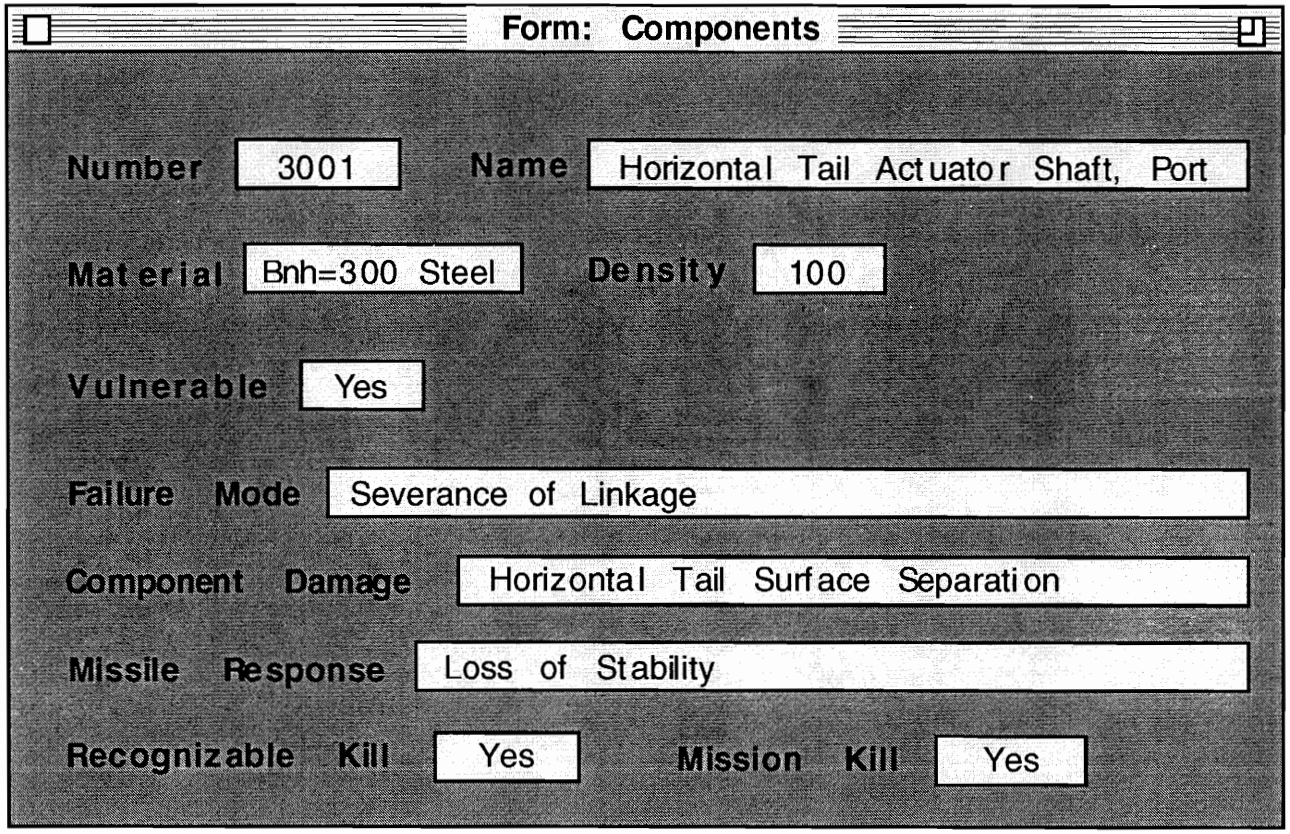


Figure 2.2. Sample Database Record

The remaining input files for COVART are generated as formatted reports from the component database and are then transferred to the server directory via the personal computer and terminal emulation. At this time a peer review with the other vulnerability analysts should take place. The geometric computer model, Pd/h curves, shotlines, and input files should be presented and checked by as many analysts as possible. The appropriate changes should be made before proceeding to the next step.

COVART is executed from the personal computer in terminal emulation mode using the geometric computer model, Pd/h curves, shotlines, and input files. COVART calculates vulnerable areas for twenty-six aspects about the missile.

The vulnerability of the missile has now been quantified for cube fragments between 15 and 1000 grains traveling at velocities between 1000 and 15000 ft/s. These parameters are typical, but can be varied for shape, material, mass, and velocity. The data should be checked in at least two ways. First, vulnagrams should be generated. Vulnagrams are color-coded pictures of the geometric models with the highly vulnerable areas showing up in red. The capability to draw these pictures is included with COVART. These should be examined to see whether they make sense to the vulnerability analyst. Second, the vulnerable area tables (output files from COVART) should be printed for at least three of the views. The tables should be examined for trends. Particular attention needs to be paid to discontinuities of values in the tables and to a reduction in vulnerable areas for higher fragment masses and velocities. Both scenarios are possible, but the analyst needs to make sure that the numbers are correct and that the input to COVART contained no errors.

The data is now distributed to customers. Distribution of data can be through electronic mail or courier, depending on the security classification of the material.

AutoCAD and Fox Pro are two commercially-available software packages that would be compatible with the automated target vulnerability quantification process. They

are very popular, well-tested, and satisfy the needs of the system. A case can be made for another CAD or database software package if it offers a lower cost solution or can more appropriately satisfy the needs of the system.

2.3 Performance and Physical Parameters

2.3.1 System

The overall system design goal is to reduce the time required to perform a single target vulnerability quantification while maintaining the same level of accuracy. The time to quantify the vulnerability of a missile shall be reduced from 52 weeks to 38 weeks. Geometric computer descriptions shall reflect intelligence drawings and contain zero modeling errors. The component database shall reflect the latest intelligence information exactly. All assumptions that are made shall be clearly documented within the database. COVART input data shall contain zero errors.

2.3.2 Software

New software shall be used on IBM compatible, and Macintosh computers. CAD software must be capable of supporting files containing 2000 components with excellent error-checking capabilities. Database software must be capable of supporting files containing 2000 records with 15 fields per record. Software must be well-tested and well-documented. Development of specialized software such as FATEPEN, FASTGEN, and COVART will continue via contractor, who will incorporate the results of the latest test data into the computer code. These represent minimum requirements.

2.3.3 Hardware

Current personal computers (Pentium and Power Macintosh) shall have a minimum of 24 Mb of RAM and 250 Mb of free disk space to perform all phases of the target vulnerability quantification. The server shall represent a six-fold improvement in running time per job over the previous generation of server. Network hardware such as hubs and ethernet cable shall be purchased for the new system.

2.4 Use Requirements

The system server and network will be available for continuous usage (24 hours a day, all year long). However, an assumed average usage will be considered as 40 hours per week per vulnerability analyst. 5 analysts will be capable of using the system at the same time through all system phases. Licenses shall be obtained for all applicable software.

2.5 Operational Deployment

For the purpose of the target vulnerability quantification system, G24 shall hire a full-time vulnerability analyst with a background in computer science. He shall be experienced in the use of CAD and database software. He shall be knowledgeable in file and data management. The hiring process shall take four weeks.

The necessary system software is currently available through mail order and numerous retail stores. The three most popular versions, by sales volume, of CAD and database software shall be judged based on compatibility, ease of use, documentation and cost by the vulnerability analysts. The best CAD and database software shall be chosen from these versions. Five copies of CAD software, and five copies of database software

will be loaded onto the hard drives of existing personal computers. This process will require four weeks.

A new AlphaServer 200/166 MHz, also currently available, shall be ordered and installed in the place of the previous server. The acquisition and installation of the server shall take four weeks.

Software training will be on-the-job with assistance provided by the new analyst. Since the server will be purchased from the same company as the previous server, commands and operating procedures will be comparable. Therefore, only minor training will be required in regard to server usage. Training for the vulnerability analysts shall take four weeks.

All equipment and training will be deployed at NSWCDD in Dahlgren, VA. The system will become fully operational in February 1997.

2.6 Operational Life-Cycle

The system should have a life expectancy of 5 years with potential software updates after two years and regular system maintenance. The 5 years represent the technology turn over in computer software and hardware. The change in cost from the current system to the automated system including hardware, software, maintenance and training should not exceed $50,000.

2.7 Effectiveness Factors

The automated system must reduce the time required to quantify the vulnerability of targets. The importance of timely assessments has been established in section 1.3. As a result of increased output and the salaries remaining fairly constant, the salary value of

increased productivity should compensate, over the life-cycle, for the acquisition costs and time lost in training.

2.8 Environment

The system will be located in a climate controlled environment, and will operate in temperatures from 50 °F to 80 °F.

3.0 Maintenance Concept

The target vulnerability quantification system consists of several important elements including analysts, hardware, and software. The objective of the maintenance concept is to formulate a plan for how the system elements will be supported on a life-cycle basis. This concept represents the most likely approach envisioned now, and it will be updated as system development progresses. The maintenance responsibilities are divided into three categories: organizational maintenance, intermediate maintenance, and depot maintenance.

3.1 Organizational Maintenance

The organizational maintenance function is performed at the location of the prime equipment in Dahlgren, VA. The vulnerability analysts are the end users of the quantification system. The maintenance tasks that the end users perform are minor equipment cleaning, and limited equipment adjustments. These activities include periodically removing dust from hardware, ensuring the proper temperature in the operating environment and inspecting cables and hard-point connections.

Additionally, end users monitor the equipment performance. As new versions of system and application software become available, end users will be responsible for determining whether the upgrades are worthwhile investments for the system. End users perform any necessary software installations. They also perform weekly backups to ensure the safety and availability of the target vulnerability data.

The procedures for carrying out these tasks are described in user manuals supplied by the hardware and software manufacturers. These manuals give the criteria for determining whether equipment or software is not functioning properly, as well as

procedures that the end user can perform to troubleshoot the problem. The manuals also identify hardware components that end users should not attempt to repair.

The vulnerability quantification system maintains a supply of spare parts and the equipment required to perform minor maintenance tasks. The equipment and parts for performing these tasks is stored at Dahlgren and are periodically reordered, as usage demands, from the product distributor. Specifically, the on-site stored parts include an assortment of cables, connection boxes, and terminators, as well as toner cartridges and paper for printers. Dahlgren also maintains a supply of tools for minor maintenance tasks such as screw drivers, needle-nose pliers and so on. These items are on hand to reduce the amount of potential system downtime.

3.2 Intermediate Maintenance

The intermediate maintenance function is performed at the Dahlgren site by a mobile intermediate technical representative of the product distributor. This technician provides support equipment needed to perform fault isolation on any system element. The maintenance tasks that the technician performs are regularly scheduled detailed inspections and major equipment repairs. These activities include inspections that are more sophisticated than organizational-level maintenance. Additionally, the technician is on call to perform major repairs to hard drives, power supplies and other components. The technician is tasked with isolating the fault and either replacing the malfunctioning item with a spare or repairing the faulty component. Items that cannot be repaired at this level are sent to the depot maintenance facility for repair or disposal if repairs are not possible.

The mobile intermediate technician does not maintain a supply of major system components such as power supplies for use as replacement parts. Most system components, however, are available from a product distributor within 24 hours. Most of

the maintenance performed by the intermediate technician involves tasks that end users cannot accomplish because they lack the proper inspection equipment, test equipment, or skills.

3.3 Depot Maintenance

The depot maintenance function is performed by the system equipment producers. Repairs too complex to be performed at Dahlgren are done at their sites. The depot locations depend on the location of the company selected to supply each specific system component. The depot sites have the most complex test and support equipment. The depot sites have the highest skilled personnel available for fault isolation. These personnel are responsible for performing diagnostics and repairs that intermediate level personnel cannot because they lack the specialized equipment or skills. The depot sites also supply the intermediate sites with the spare parts they require.

If a depot site determines that a component is worth repairing, its personnel make the appropriate repairs and return the item to the system in Dahlgren. If the component is not worth fixing, it is disposed of properly.

4.0 Functional Analysis

A condensed functional analysis is done to show the design requirements for the target vulnerability quantification system. Figures 4.1, through 4.3 illustrate the operational functional flow to three levels. These figures are derived from the operational requirements. Figure 4.4 illustrates the maintenance functional flow. It is derived from the maintenance concept.

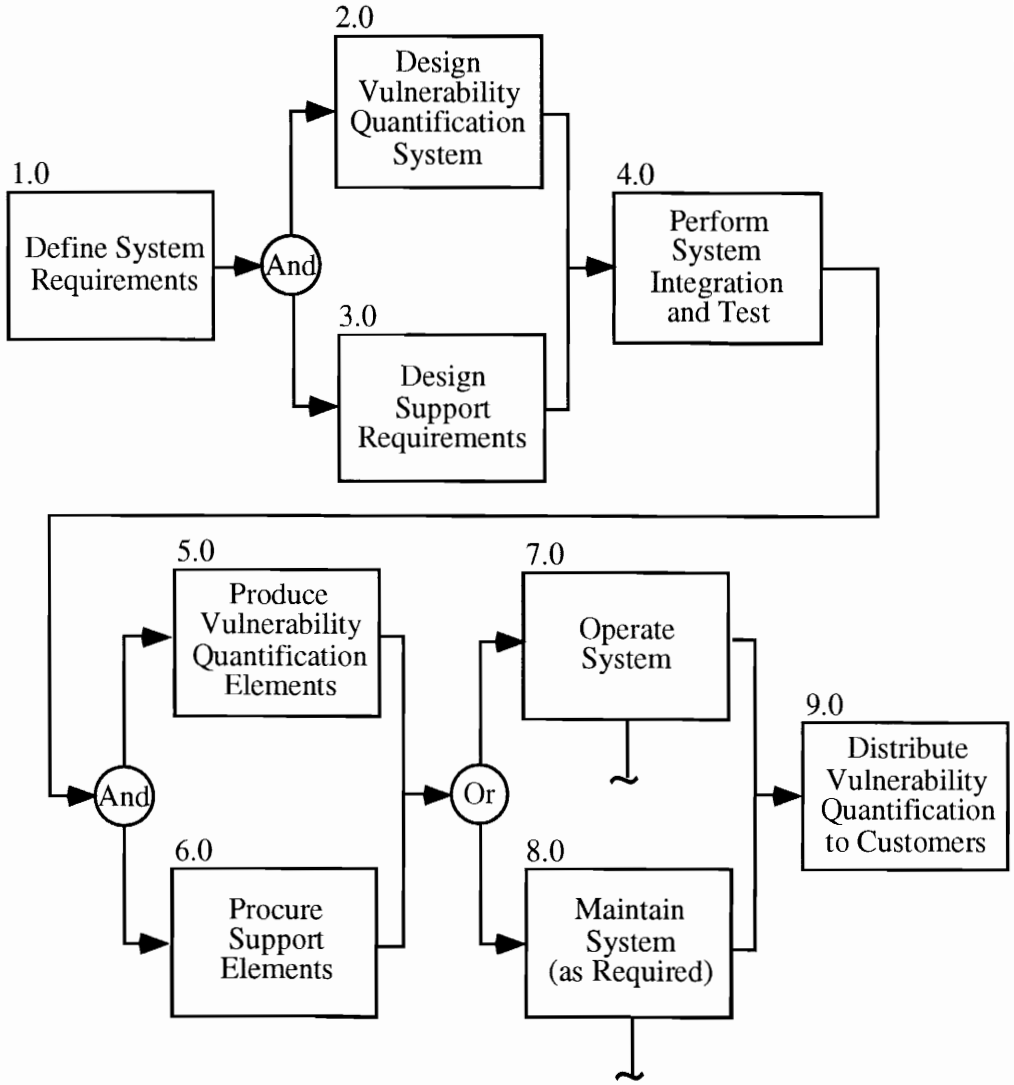


Figure 4.1. First Level Operational Flow

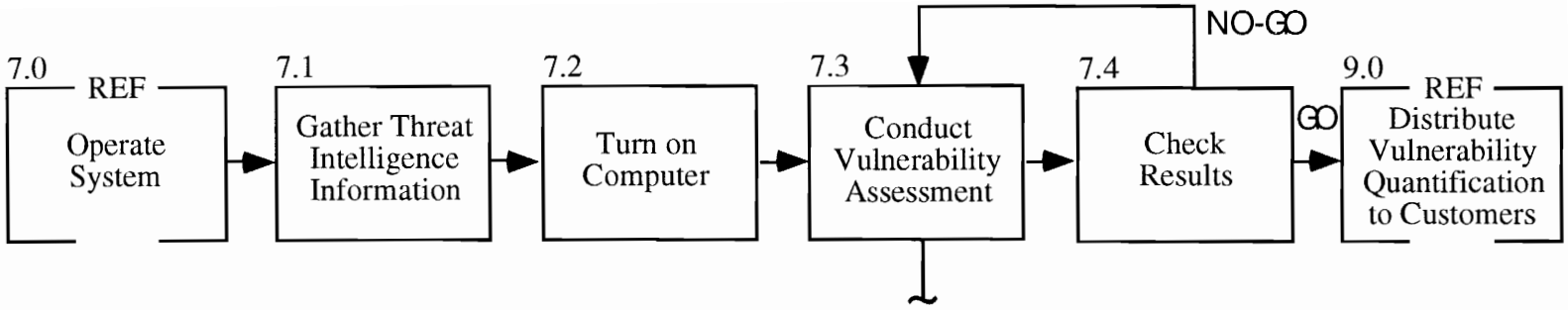


Figure 4.2. Second Level Operational Flow

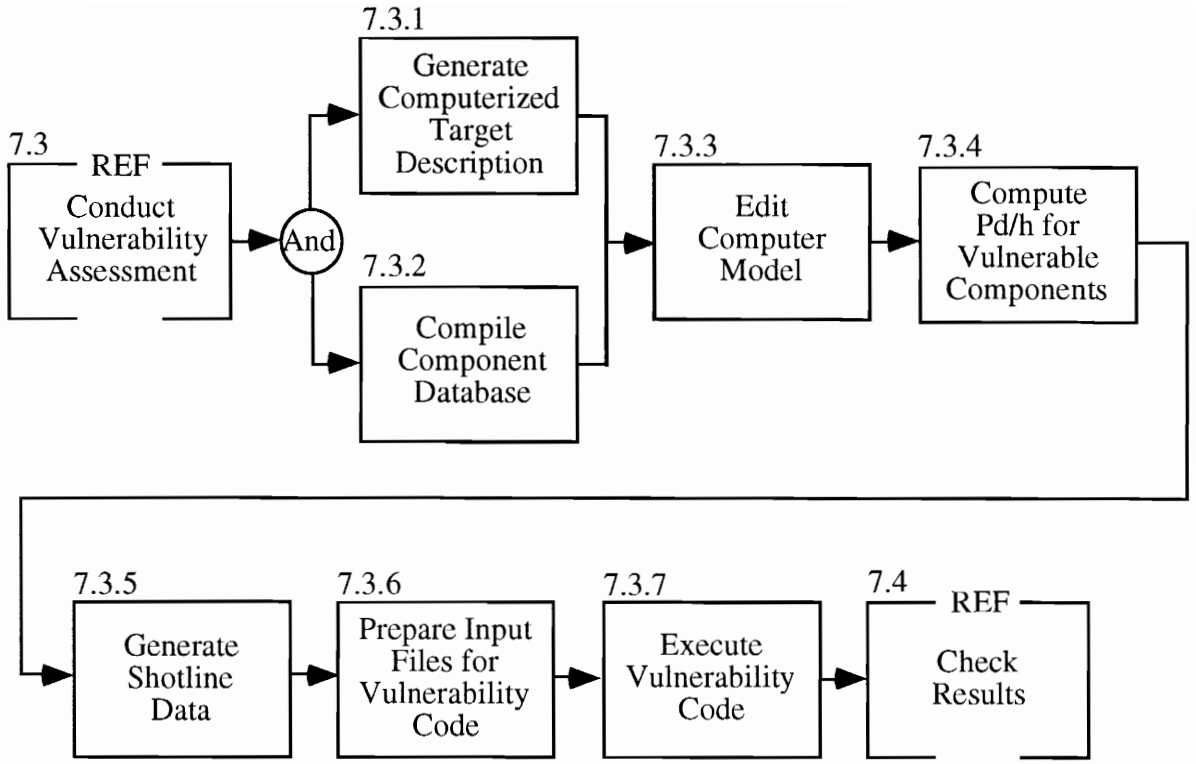


Figure 4.3. Third Level Operational Flow

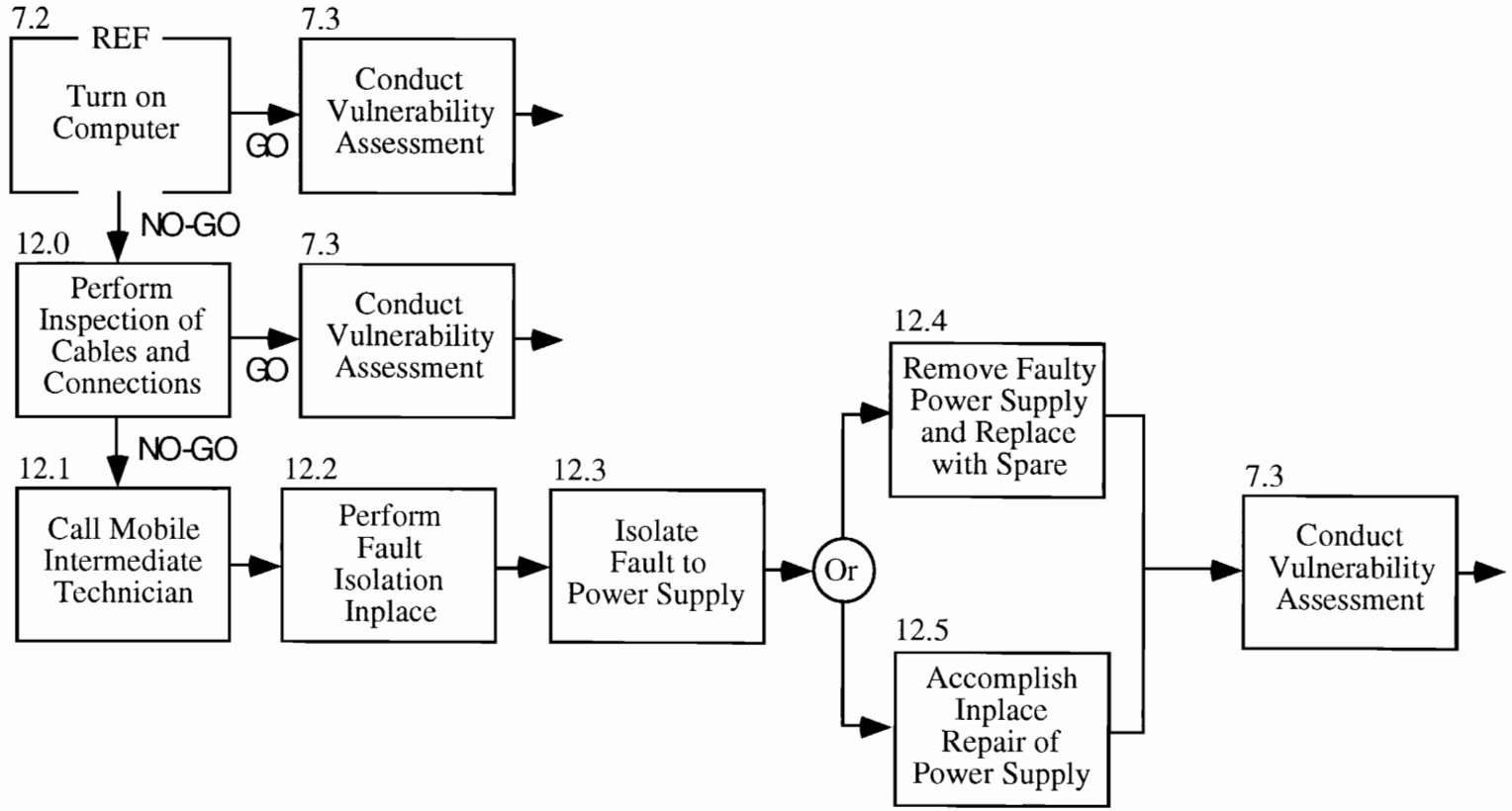


Figure 4.4. Maintenance Flow

5.0 Conceptual System Design

5.1 Vulnerability Quantification System Architecture

Figure 5.1 illustrates the vulnerability quantification system architecture. The main system components shown are the personal computers, hubs, laser printer, and AlphaServer. The necessity of these hardware elements evolve from the third level operational flow diagram (Figure 4.3).

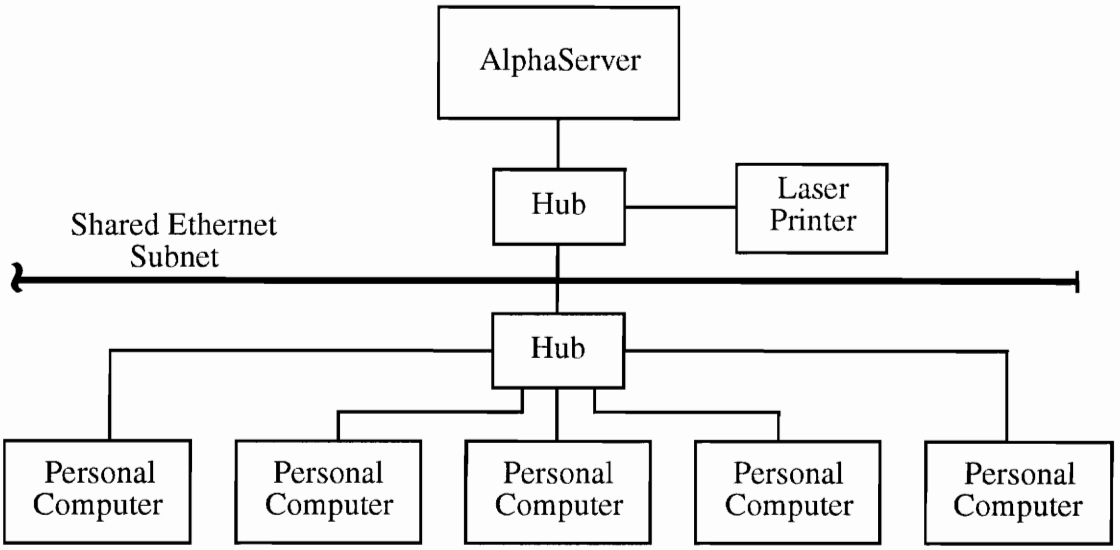


Figure 5.1. Vulnerability Quantification System Architecture

As Figure 4.3 shows, the vulnerability analyst constructs the computer model and component database from intelligence data at his personal computer, using CAD and database software loaded on his computer's hard drive. In this system setup, there is one IBM-compatible PC and four Power Macintosh computers. The CAD and database software run native on the individual computers. After the computer model has been

edited, the component Pd/h curves are calculated using the FATEPEN vulnerability code. This software is also preloaded on each personal computer. FATEPEN can be run native on IBM-compatible PCs or via SoftWindows on Macintosh computers. Next, the input files for COVART are generated as reports from the database software. Subsequently, the computer model, COVART input files, and Pd/h curves are transferred from the hard drive of the personal computer to a working directory on the AlphaServer via Fetch. The shared ethernet makes these large file transfers in seconds. Using VersaTermPro, the analyst logs on to the AlphaServer 200/166Mhz. His computer now acts as a dummy terminal with the VAX operating environment. The AlphaServer contains the latest versions of the FASTGEN and COVART vulnerability codes. While his computer is in terminal emulation mode, the vulnerability analyst generates the shotline data file using FASTGEN, checks the input files, and executes COVART. Before COVART is executed, however, the input data should be presented in an informal peer review. Data from COVART is output to the laser printer for checking. Finally, the product is distributed to customers.

5.2 Requirements Allocation

Figure 5.2 illustrates the life-cycle functional requirements and allocation. The top-level system elements of analyst, hardware and software are broken down into the hardware and software units. Figure 5.2 evolves from the functional analysis and the system architecture. The costs are for the five year life-cycle and are expressed in 1997 dollars. Network equipment consists of the acquisition and maintenance costs for the laser printer, ethernet hubs and ethernet cables. The support software includes Fetch, SoftWindows and VersaTermPro. The cost estimates are conservative. They include the potential of adding upgrades to the system when they are deemed necessary.

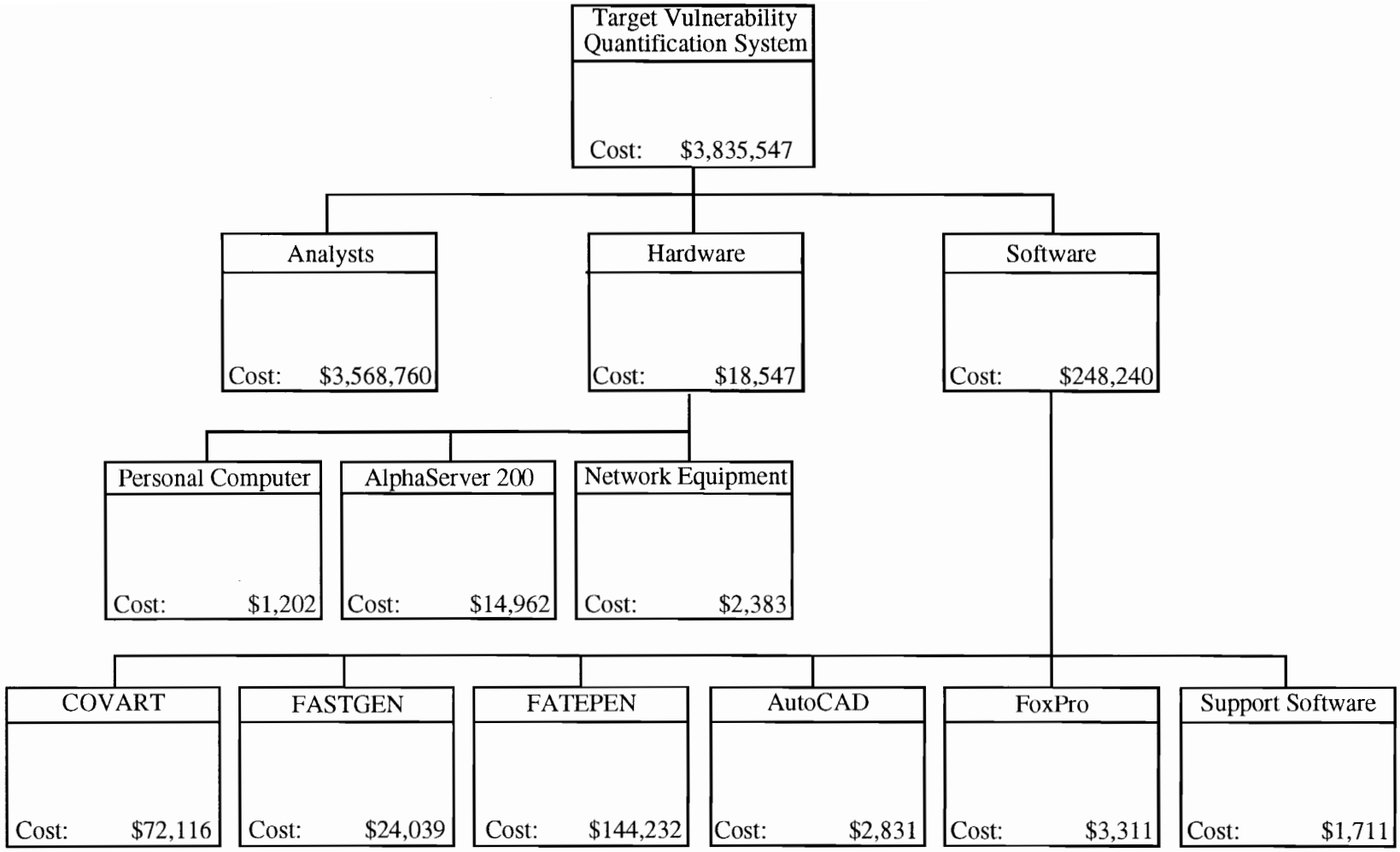


Figure 5.2. Life-Cycle Functional Requirements and Allocation

5.3 Cost Analysis

A cost analysis is an important consideration for the new system (Figure 5.3). The automated system must be capable of producing the desired result of reducing the time required to perform the vulnerability quantification. However, the cost of any new system cannot become prohibitively expensive. For example, a new system can be designed to produce twice as many assessments as the current system, but the assessments may cost twice as much to perform.

Salaries are the largest expense for the system. In both the current and automated systems, the yearly salaries for the five analysts remain the same. To implement the automated system, however, time must be devoted to training the analysts. Four weeks of training for five analysts (in only the first year) are equivalent to an additional salary expense of $54,904. That is, $54,904 worth of time is spent in training and not performing assessments. The payoff comes in that the five analysts can complete almost two extra assessments per year (Table 5.1). This increase in productivity amounts to a savings of $29,740 in the first year and increases each year thereafter. This essentially amounts to a reduction in salary cost per assessment.

Hardware acquisition costs are incurred only for the automated system. The cost in the first year of a new server, ethernet cable, and ethernet hubs is $14,460. A side-by-side comparison of the hardware maintenance costs shows that a savings is achieved by implementing the automated system. A costly ($2,000 per year) maintenance contract for the current microcomputer can be dropped, and an annual savings of $1,800 can be realized.

Software acquisition costs are incurred only for the automated system. In the first year, $4,970 is spent to procure new software for five analysts, and $3,000 is allocated for

	1997		1998		1999		2000		2001	
	Current	Automated	Current	Automated	Current	Automated	Current	Automated	Current	Automated
Salary Costs										
Analysts (5)	713,752	713,752	728,027	728,027	742,588	742,588	757,439	757,439	772,588	772,588
Salary value of time spent in training		(54,804)		-		-		-		-
Salary value of increased productivity		29,740		39,201		39,985		40,785		41,601
Total Salary Costs	713,752	738,916	728,027	688,826	742,588	702,602	757,439	716,654	772,588	730,987
Change in Salary Costs		25,164		(39,201)		(39,985)		(40,785)		(41,601)
Hardware Acquisition Costs										
Power Macintosh 7100/66Av	-	-	-	-	-	-	-	-	-	-
Power Macintosh 9500/132	-	-	-	-	-	-	-	-	-	-
Power Macintosh 7100/80Av	-	-	-	-	-	-	-	-	-	-
Power Macintosh 7100/80Av	-	-	-	-	-	-	-	-	-	-
Gateway 2000 P5-90	-	-	-	-	-	-	-	-	-	-
Laser printer	-	-	-	-	-	-	-	-	-	-
MicroVax 2	-	-	-	-	-	-	-	-	-	-
AlphaServer 200/166Mhz		14,000		-		-		-		-
Asante ethernet hub		400		-		-		-		-
Ethernet cable		60		-		-		-		-
Total Hardware Acquisition Costs	-	14,460	-	-	-	-	-	-	-	-
Change in Hardware Acquisition Costs		14,460		-		-		-		-
Hardware Maintenance Costs										
Power Macintosh 7100/66Av	50	50	50	50	50	50	50	50	50	50
Power Macintosh 9500/132	50	50	50	50	50	50	50	50	50	50
Power Macintosh 7100/80Av	50	50	50	50	50	50	50	50	50	50
Power Macintosh 7100/80Av	50	50	50	50	50	50	50	50	50	50
Gateway 2000 P5-90	50	50	50	50	50	50	50	50	50	50
Laser printer	400	400	400	400	400	400	400	400	400	400
MicroVax 2	2,000		2,000		2,000		2,000		2,000	
AlphaServer 200/166Mhz		200		200		200		200		200
Asante ethernet hub		-		-		-		-		-
Ethernet cable		-		-		-		-		-
Total Hardware Maintenance Costs	2,650	850	2,650	850	2,650	850	2,650	850	2,650	850
Change in Hardware Maintenance Costs		(1,800)		(1,800)		(1,800)		(1,800)		(1,800)
Software Acquisition Costs										
COVART	-	-	-	-	-	-	-	-	-	-
FASTGEN	-	-	-	-	-	-	-	-	-	-
FATEPEN	-	-	-	-	-	-	-	-	-	-
VersaTermPro	-	-	-	-	-	-	-	-	-	-
AutoCAD (5)		1,870		-		1,000		-		-
Fetch		-		-		-		-		-
FoxPro (5)		2,350		-		1,000		-		-
SoftWindows (2)		750		-		1,000		-		-
Total Software Acquisition Costs	-	4,970	-	-	-	3,000	-	-	-	-
Change in Software Acquisition Costs		4,970		-		3,000		-		-
Software Development Cost										
COVART	15,000	15,000	15,000	15,000	15,000	15,000	15,000	15,000	15,000	15,000
FASTGEN	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000
FATEPEN	30,000	30,000	30,000	30,000	30,000	30,000	30,000	30,000	30,000	30,000
Total Software Development Costs	50,000	50,000	50,000	50,000	50,000	50,000	50,000	50,000	50,000	50,000
Change in Software Development Costs		-		-		-		-		-
Total Costs	**766,402**	**809,196**	**780,677**	**739,676**	**795,238**	**756,452**	**810,089**	**767,504**	**825,238**	**781,837**
Change in Total Costs		**42,794**		**(41,001)**		**(38,785)**		**(42,585)**		**(43,401)**
Change in Costs (1997 Dollars)		**(114,907)**								

Figure 5.3. Side-by-Side Cost Comparison

Table 5.1. Productivity Analysis

	1997	1998	1999	2000	2001
Current System					
Weeks required to complete assessment	52	52	52	52	52
Number of assessments completed per year	5.00	5.00	5.00	5.00	5.00
Total annual salary cost	$ 713,752	$ 728,027	$ 742,588	$ 757,439	$ 772,588
Salary cost per assessment	$ 142,750	$ 145,605	$ 148,518	$ 151,488	$ 154,518
Automated System					
Weeks required to complete assessment	38	38	38	38	38
Number of assessments completed per year *(not adjusted for time spent in training)*	6.84	6.84	6.84	6.84	6.84
Number of weeks spent in training	4	-	-	-	-
Total annual salary cost	$ 713,752	$ 728,027	$ 742,588	$ 757,439	$ 772,588
Salary value of time spent in training	$ 54,904	$ -	$ -	$ -	$ -
Salary cost per assessment	$ 104,318	$ 106,404	$ 108,532	$ 110,703	$ 112,917
Salary value of increased productivity	**$ 29,740**	**$ 39,201**	**$ 39,985**	**$ 40,785**	**$ 41,601**

potential upgrades in two years thereafter. Finally, specialized software development costs are the same for both systems.

To summarize, by reducing the time required to complete the target vulnerability quantification, the productivity (output) is increased. Because the salaries remain fairly constant, the salary value of increased productivity compensates, over the life-cycle, for the acquisition costs and time lost in training.

6.0 Conclusions

The purpose of this report was to demonstrate the application of the systems engineering methodology in redesigning the target vulnerability quantification process. The need to redesign arises from the Navy's requirement to defend military and civilian assets around the world. The sooner NAVSEA, NAVAIR, warhead developers, and endgame modelers can update their systems with the vulnerability quantification data, the more effectively the Navy can operate.

Analysts, hardware, and software comprise the target vulnerability quantification system that produces vulnerable areas for missile and aircraft targets. The functions that are required to perform the process are identified. They include constructing computer descriptions and formatted input files to COVART for the target. Off-the-shelf hardware and software alternatives that will assist in reducing the time to perform the system functions are examined. The software includes CAD and database packages, and the hardware includes an AlphaServer 200 that will improve the processing speed six-fold over the current system.

The conceptual design presented in this paper shows the basic system components and their arrangement. Design features such as formatting COVART input files from database files will, in effect, automate much of the current process. By having the computer generate these files, the potential for data entry errors and the amount of time spent checking errors is reduced. Additionally, automation will reduce the time required to perform the process by reducing the number of hand calculations required in designing computer models.

The cost analysis shows that the cost per assessment goes down in the automated system. The automated system reduces the time required to complete each assessment, which increases the productivity of the analysts. The salary value of increased productivity

more than compensates for the acquisition and training costs incurred with the automated system.

6.1 Recommendations

The need for a timely, accurate target vulnerability quantification system is real. Fierce competition for defense dollars exists. G24 must look at other automation and system integration techniques to improve the process and to meet the needs of the Navy. This may include further automation of the Pd/h curve development process, and modifying COVART to accept database information directly.

The ways in which the analysts are utilized should be further investigated. The functions performed or the skills required by a computer scientist should be reviewed.

The cost of poor quality needs to be studied in the case of the current system and in the case of the automated system. For example, if a mistake is detected in the check results box of the operational flow diagram, how does this affect the time, and subsequently, the productivity and cost of the analyses?

Finally, the idea of continuously improving the process needs to be fostered in the group. Placing the focus on quality, will eventually increase the productivity of the process.

Bibliography

Ball, Robert E. *The Fundamentals of Aircraft Combat Survivability Analysis and Design.* New York: AIAA, 1985.

Batra, D. "A Framework for Studying Human Error Behavior in Conceptual Database Modeling." *Information & Management* 25, no. 3 (September 1993), p121-131.

Blanchard, Benjamin S., and Wolter J. Fabrycky. *Systems Engineering and Analysis.* Englewood Cliffs, NJ: Prentice Hall, 1990.

Brigham, Eugene F., and Louis C. Gapenski. *Financial Management, 7th ed.* Fort Worth: Dryden Press, 1994.

Cushman, William H., and Daniel J. Rosenberg. *Human Factors in Product Design.* Amsterdam: Elsevier, 1991.

Frieden, David R., ed. *Principles of Naval Weapons Systems.* Annapolis, MD: Naval Institute Press, 1988.

Garvin, David A. *Managing Quality.* New York: The Free Press, 1988.

Juran, J.M., Frank M Gryna. *Quality Planning and Analysis.* New York: McGraw-Hill, 1993.

McMahon, Chris, and Jimmie Browne. *CAD CAM From Principle to Practice.* Wokingham, England: Addison-Wesley, 1993.

Triantis, Kostas. Class notes for Management of Quality and Reliability (ISE5124). Falls Church, VA: Virginia Tech, 1995.

A. Quality and the Target Vulnerability Quantification Process

The productivity of any process can be improved through Total Quality Management (TQM). Currently, the quantification process is performed with little or no attention to quality measures. The word *quality* does not appear in the mission statement of the branch, and the process lacks quality checks. There is general skepticism of TQM in the group.

A.1 Quality Mission

The current mission statement for G24 is

The Lethality and Weapons effectiveness branch

- *Assesses the vulnerability of foreign aerial targets (manned and unmanned) to damage by conventional kill mechanisms*
- *Assesses the terminal effectiveness of current and conceptual tactical missile systems against a variety of manned aircraft, anti-ship cruise missiles, theater ballistic missiles, and strike warfare threats*
- *Examines the effects on weapon system effectiveness of various design alternatives (such as warhead or fuze options) through the use of performance studies*
- *Develops and maintain mathematical models and methodologies*
- *Conducts penetration and component/system lethality testing for inputs to vulnerability models*

Quality has not been addressed in this mission statement. Likewise, the mission statement is not well known among the members of G24. It is merely a public relations tool used by the branch head to advertise G24 to the defense community as a way to secure continued funding.

A.2 Customers

To create quality products, the vulnerability analysts must recognize who their customers are and how they will use the product. Vulnerability analysts must work in conjunction with their customers. Data should be output in a format that is compatible with their customers' systems. The vulnerability process must be flexible enough to meet these demands.

The customers include the Naval command structure (NAVSEA and NAVAIR), who develop defensive weapon systems and who are responsible for target selection. These customers use the vulnerability information to make managerial decisions and to initiate system changes and upgrades. Their primary concern is the adequacy of the current defensive systems. Warhead developers are also customers. They work iteratively with vulnerable data to design and update warhead configurations. Finally, fleet engagement wargame modelers use vulnerability data. These customers use vulnerability information to model fleet engagements of multiple targets. Their primary concern is whether the US will win encounters with the enemy and, if not, what must be done to correct the situation.

A.3 Dimensions of Quality

The dimensions of quality are performance, reliability, conformance, serviceability, aesthetics, perceived quality, and durability.

Performance describes the primary operating characteristics of the product. Performance is based on how well the needs of the customer are met. High performance is represented by a process that continuously keeps the customer's needs in mind.

Reliability involves the quality checks within the system. It tracks whether appropriate real-life tests are in place to check the vulnerability assessment. For example,

Pd/h results computed by FATEPEN are often evaluated against test data. Other reliability checks include formal peer reviews.

Conformance is the degree to which the product's operating characteristics meet the established specifications. In this case, it is the degree to which the vulnerability assessment conforms to the customer's needs. COVART output (vulnerable area tables) are formatted to match the customer's data needs. Likewise, internal quality standards should be met. Analyst generated computer descriptions should be modeled in a predictable fashion throughout the process. For example, port refers to the pilot's left and is represented by positive y values; starboard refers to the pilot's right and is represented by negative y values. Therefore, conformance implies consistency within the process.

Serviceability is a factor of speed, competence, and response to customers needs. In this sense, serviceability measures how well the comments of customers are received in the process.

Aesthetics, or how a product looks is not as important as other dimensions, but it still plays a role. How the vulnerability assessment is presented such as through graphics and text, helps the customer understand and use the results.

Perceived quality relates to the way customers feel about a product and the process from which it was created. Because computer simulation is much less expensive than actual testing, it is feasible to validate only certain aspects of the process through testing. The customers must have faith in the process often without validation from testing. If the process produces consistently accurate vulnerability assessments confirmed through testing, customers will trust the vulnerability assessments even when they are not verified through testing. A good indication of perceived quality is whether the customers are satisfied with the quality of service.

Durability has little relevance to this process because the product is not subject to wear.

A.4 Malcolm Baldrige Quality Criteria

The Malcolm Baldrige Quality Award is used as the standard to develop the quality criteria for the vulnerability quantification process. The Baldrige criteria are used across industries as the basis for determining awards and for providing constructive feedback to the applicants. For this paper, the criteria have been modified so that they are applicable to the vulnerability assessment process. They also combine the dimensions of quality discussed in section A.3.

A.4.1 Leadership

The first criterion is the leadership system, which includes strategic directions and expectations. It examines how the leadership sets the goals and direction of the organization and how these goals are effectively communicated to individuals. In this process, the senior executive is the branch head. The leadership is responsible for writing the mission statement and for interacting with the Naval command structure. Also, leadership supplies administrative support including, evaluating and rewarding employees, and ensuring an appropriate work environment.

A.4.2 Information and Analysis

The information and analysis criterion measures how the data and information is managed and used throughout the organization. The vulnerability assessment relies on a database of many years of testing and analysis, which is manifest in the COVART and FATEPEN vulnerability codes. Because it is cost-effective to build on what has been previously developed, it is vital that this in-house vulnerability database be maintained and adequately serviced by the organization. It must be available and promoted for use by all

employees. The information and analysis criterion also addresses how information is shared among individuals to maintain continuity if someone is ill or quits.

A.4.3 Strategic Planning

The strategic planning criterion examines how the organization sets strategic directions and how requirements are translated into an effective performance management system. For the vulnerability assessment process, this includes the mission statement, quality mission, and how they are disseminated to G24.

A.4.4 Human Resource Development and Management

The human resource development and management criterion measures how the organization develops and maintains a work environment that encourages personnel growth. It examines how the organization rewards employees through compensation and recognition. It also determines whether work and performance evaluations are designed to allow for a reward system. Another component explores how the organization develops the work force through education and training on an ongoing basis. Finally, the criterion measures employee satisfaction and well-being and how employees are effected by changes in the work environment.

A.4.5 Process Management

This criterion examines process management, including support services. The process is examined to determine whether the tools necessary for a quality product are in place. For example, the computer used by an analyst is vital to him during his vulnerability assessment. For the most efficient workplace, the computer codes need to be user-

friendly. The support services are examined to determine how they work in conjunction with the employee.

A.4.6 Customer Focus and Satisfaction

The customer focus and satisfaction criterion looks at how the organization determines customer satisfaction and how it uses this information to build and improve customer-organization relationships. It considers, for example, whether the individual employee knows who the customer is and what his needs are. Quality is based on how well the output from the vulnerability process meets the customer needs and how appropriate it is to the Naval command.

A.4.7 Interrelationships Between Criteria

At NSWCDD, the leadership is structured to supply administration for the group, as well as supplying technical leadership. Branch heads are responsible for administrative and technical leadership. In G24, the branch head as a technical leader interacts with Naval command. He also does strategic planning and signs off on employee performance reviews, promotions and awards. The branch head meets with external customers to ensure their satisfaction and to convince them to continue using G24 services. Ultimately, the branch head effects the level of quality.

A.5 Quality Survey

The instrument selected to rank quality in G24 was a 28-item internal survey with a Likert-type response format with responses ranging from strongly agree to strongly disagree. The response format is presented at the end of Appendix A.

Sixteen surveys were completed by G24 employees. The survey statements and results were grouped by their corresponding quality dimension and are presented at the end of Appendix A.

An average score and standard deviation were computed separately for each quality dimension or criterion. These results are summarized in Table A.1. The lowest scores came in internal serviceability and leadership, which were 1.81 and 2.08 respectively. Internal serviceability could be improved by developing a process to manage workloads when an employee gets sick or quits.

Table A.1. Summary of Results

Quality Dimension or Criteria	Average Score	Standard Dev.
Performance	3.50	0.82
Reliability	3.09	0.96
Conformance	3.50	0.82
Serviceability	3.69	0.79
Internal Serviceability	1.81	0.91
Perceived Quality	3.47	0.72
Leadership	2.08	1.09
Information	2.80	1.01
Strategic Planning	2.38	1.02
Human Resources	2.92	1.11
Process Management	2.63	1.06
Customer Focus & Satisfaction	3.47	0.80

Quality begins at the top, and this survey indicates a lack of effective communication and involvement in the target vulnerability process by the branch head. Improving communications between management and employees is essential in a quality organization. Employees should be able to depend on management for important news; however, this is clearly not the case. Important news travels almost exclusively through the office grapevine. While the office grapevine may never be equaled in terms of speed, open and forthright communication is the only means for preventing rumors and their deleterious effects to morale and productivity.

Employees gave the branch high marks in performance, conformance, serviceability, perceived quality, and customer focus and satisfaction.

Employees seem comfortable with their relationships to their customers, the feedback they receive, and the speed and accuracy of answering customer questions. Figure A.1 presents these quality dimension scores graphically. Figure A.1 shows that the maximum score is 3.69. This demonstrates that there are definitely areas for improvement.

A.6 Quality Improvement Goals

The basic assumption in any quality improvement program is that productivity and profitability will eventually increase once quality measures have been implemented. Training in TQM will help the employees of G24 understand this principle. Quality checks must be included throughout the process. This should involve the formation of discussion groups to evaluate everything from system hardware and software to data output at various stages in the process. Several improvement goals are listed below. However, the idea that a process can and should be continuously improved should not be lost.

The results of the survey point to leadership as the primary quality criterion that needs improvement. The branch head faces an imposing set of technical, managerial, and administrative responsibilities. He has a responsibility to change the quality management system of G24. Goals should include improving communication by encouraging an open dialogue between analysts and the branch head. A quality mission should be defined and discussed among all G24 personnel. The introduction of a pay-for-performance program could also enhance quality.

Contingency planning for extended employee absences due to illness, training, and so on, needs to be established. An organizational matrix with cross-training among

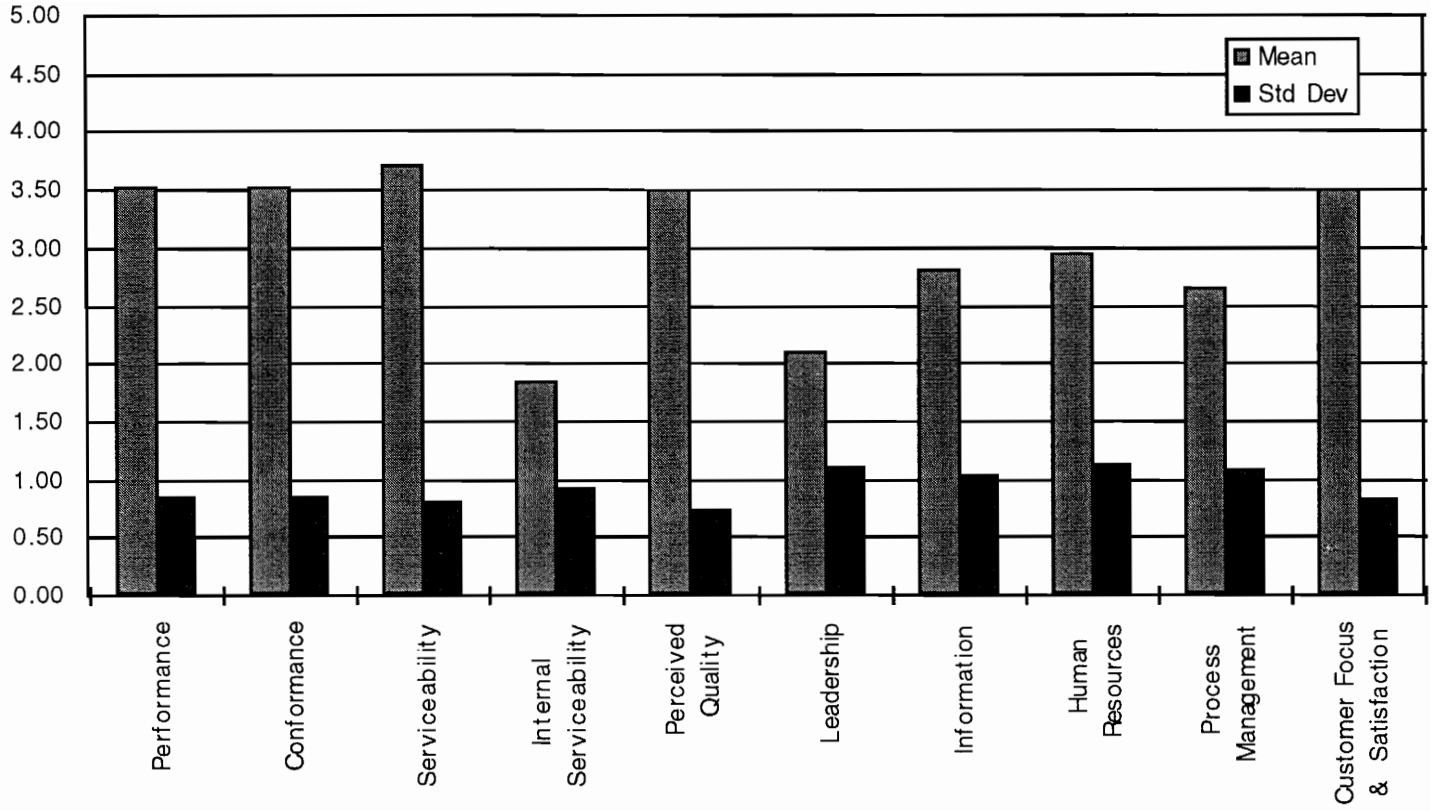


Figure A.1. Response Mean and Standard Deviation

employees should be developed. This might include formal and informal mentoring between junior and senior analysts with a special emphasis on retaining the skills and knowledge of those employees nearing retirement.

Finally, the process must incorporate computer codes that are user-friendly, and configuration management must be established to ensure process and product consistency.

TARGET VULNERABILITY GROUP (G24) SURVEY

Please read each statement and record your reaction to it as:

1 Strongly agree
2 Disagree
3 Neutral
4 Agree
5 Strongly agree

I know who the customers are and what they need.	1	2	3	4	5
A system of checks is in place to ensure a quality product.	1	2	3	4	5
Pd/h results are evaluated against test data.	1	2	3	4	5
Customer questions are answered quickly and accurately.	1	2	3	4	5
If a duty expert gets sick or quits, the work can be quickly redistributed with no impact on quality.	1	2	3	4	5
All customers are satisfied.	1	2	3	4	5
Management effectively communicates information and goals.	1	2	3	4	5
Top management is involved in the target vulnerability quantification process.	1	2	3	4	5
Important news is reported through the official channels before the office grapevine.	1	2	3	4	5
Reference material exists on how to perform a vulnerability analysis.	1	2	3	4	5
All employees, from senior management to technicians, have access to the vulnerability database.	1	2	3	4	5
Intelligence information is accurate and updated regularly.	1	2	3	4	5
The G24 quality mission is well defined.	1	2	3	4	5
Sufficient employees are hired to handle the workload.	1	2	3	4	5

Quality measures are part of the employee evaluation process and contribute to annual bonuses/incentives.	1	2	3	4	5
I am happy with my job.	1	2	3	4	5
Employees are rewarded for a job well done.	1	2	3	4	5
I feel valued as a member of the G24 team.	1	2	3	4	5
My work is rewarding.	1	2	3	4	5
Employees have been properly trained on the equipment.	1	2	3	4	5
Corporate knowledge or institutional memory is passed on to new employees through mentoring programs and other means.	1	2	3	4	5
Training opportunities are encouraged and available.	1	2	3	4	5
Management effectively plans for training needs.	1	2	3	4	5
Cross-training methods are in place within functional groups.	1	2	3	4	5
Support personnel are in place to make paperwork easier.	1	2	3	4	5
Our computer codes are user-friendly.	1	2	3	4	5
The same computer model is used from start to finish.	1	2	3	4	5
I receive feedback from customers.	1	2	3	4	5

																	Mean	Std Dev
Performance																	**3.50**	**0.82**
I know who the customers are and what they need	4	4	3	4	4	3	4	5	2	2	3	3	4	3	4	4	3.50	0.82
Reliability																	**3.09**	**0.96**
A system of checks is in place to ensure a quality product.	1	2	3	4	3	2	2	4	1	2	4	2	4	3	3	4	2.75	1.06
Pd/h results are evaluated against test data.	2	4	3	4	3	3	4	4	2	4	3	3	4	4	4	4	3.44	0.73
Conformance																	**3.50**	**0.82**
I know who the customers are and what they need	4	4	3	4	4	3	4	5	2	2	3	3	4	3	4	4	3.50	0.82
Serviceability																	**3.69**	**0.79**
Customer questions are answered quickly and accurately.	4	3	3	5	4	3	3	4	3	4	5	3	4	3	5	3	3.69	0.79
Internal Serviceability																	**1.81**	**0.91**
If a duty expert gets sick or quits, the work can be quickly redistributed with no impact on quality.	1	1	3	2	1	2	2	1	1	1	2	2	4	3	1	2	1.81	0.91
Perceived Quality																	**3.47**	**0.72**
All customers are satisfied.	3	3	3	3	2	3	3	4	3	4	3	4	4	3	4	3	3.25	0.58
Customer questions are answered quickly and accurately.	4	3	3	5	4	3	3	4	3	4	5	3	4	3	5	3	3.69	0.79
Leadership																	**2.08**	**1.09**
Management effectively communicates information and goals.	1	1	3	4	3	2	2	3	1	2	2	1	3	4	1	4	2.31	1.14
Top management is involved in the target vulnerability process.	3	1	2	2	4	3	2	1	1	2	3	3	4	4	1	4	2.50	1.15
Important news is reported through the official channels before the office grapevine.	1	2	2	1	1	1	1	1	1	1	2	1	3	2	1	2	1.44	0.63
Information																	**2.80**	**1.01**
Reference material exists on how to perform a vulnerability analysis.	3	3	2	4	2	4	2	3	4	2	3	3	4	4	3	3	3.06	0.77
All employees, from senior management to technicians, have access to the vulnerability database.	1	4	3	3	2	3	4	4	3	2	3	3	3	3	3	4	3.00	0.82
If a duty expert gets sick or quits, the work can be quickly redistributed with no impact on quality.	1	1	3	2	1	2	2	1	1	1	2	2	4	3	1	2	1.81	0.91
Intelligence information is accurate and updated regularly.	3	4	2	4	4	4	4	3	1	4	4	3	3	3	4	3	3.31	0.87
Strategic Planning																	**2.38**	**1.02**
The G24 quality mission is well defined.	2	1	2	3	2	1	3	4	2	1	2	2	3	4	2	4	2.38	1.02
Human Resources																	**2.92**	**1.11**
Sufficient employees are hired to handle the workload.	4	5	3	3	4	3	4	3	2	4	3	4	3	4	3	5	3.56	0.81
Quality measures are part of the employee evaluation process and contribute to annual bonuses and incentives.	3	1	2	2	3	1	1	4	2	1	2	2	1	3	3	1	2.00	0.97
I am happy with my job.	4	4	2	4	4	4	2	4	3	4	4	5	3	4	5	4	3.75	0.86
Employees are rewarded for a job well done.	4	2	1	1	4	2	3	4	2	2	2	2	3	4	4	1	2.56	1.15
I feel valued as a member of the G24 team.	4	3	3	4	4	2	3	5	1	1	3	2	4	4	5	3	3.19	1.22
My work is rewarding.	4	2	2	5	4	3	2	4	4	3	4	5	3	4	5	3	3.56	1.03
Employees have been properly trained on the equipment.	2	2	3	4	4	2	4	2	2	2	3	4	3	3	3	4	2.94	0.85
Corporate knowledge or institutional memory is passed on to new employees through mentoring programs and other means.	2	1	3	4	3	2	2	2	1	1	2	2	4	4	1	2	2.25	1.06
Training opportunities are encouraged and available.	4	2	2	5	4	4	4	4	3	4	3	1	4	4	4	3	3.44	1.03
Management effectively plans for training needs.	2	2	2	3	3	3	2	3	1	4	3	1	3	2	1	3	2.38	0.89
Cross-training methods are in place within functional groups.	2	2	2	3	3	3	2	3	1	1	3	3	3	3	3	3	2.50	0.73
Process Management																	**2.63**	**1.06**
Support personnel are in place to make paperwork easier.	4	4	4	4	2	4	3	4	1	5	4	3	3	4	3	3	3.44	0.96
Computer codes are user friendly.	2	2	3	4	2	3	3	1	1	1	1	3	2	3	3	2	2.25	0.93
The same computer model is used from start to finish.	1	2	3	3	2	3	1	1	1	2	2	3	2	3	3	3	2.19	0.83
Customer Focus & Satisfaction																	**3.47**	**0.80**
All customers are satisfied.	3	3	3	3	2	3	3	4	3	4	3	4	4	3	4	3	3.25	0.58
Customer questions are answered quickly and accurately.	4	3	3	5	4	3	3	4	3	4	5	3	4	3	5	3	3.69	0.79
I receive customer feedback.	4	3	3	5	4	2	4	5	2	3	3	2	4	3	4	4	3.44	0.96
I know who the customer is and what they need.	4	4	3	4	4	3	4	5	2	2	3	3	4	3	4	4	3.50	0.82