Design of a Safety Management Information and Tracking System

By
Veronica (Randy) Tedori

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:

L. K. Harmon
L. Kenneth Harmon, Chairman

Ben S. Blanchard
Benjamin S. Blanchard Jr.

Lois A. Hennis Crawford
Lois Hennis Crawford

April, 1993
Blacksburg, Virginia

Design of a Safety Management Information and Tracking System

By
Veronica (Randy) Tedori

Committee Chairman: L. Kenneth Harmon
Systems Engineering

(ABSTRACT)

In this project, a safety management information and tracking system is designed for a particular classified military organization. The enhancements to the performance of this Government facility's safety program provided by the design will improve the history of inefficiency, which is characterized by the 1.4 million spent annually on lost time, wages and medical costs associated with accidents.

The systems engineering and analysis process is applied to create a preliminary design for an enhanced safety information system at the Government organization. The system as proposed consists of a computer based local area network and commercially available software interfacing with a bar code package and existing safety air monitoring equipment. The system is based on a streamlined version of current safety practices and processes in the Government organization. The design process includes a needs analysis, feasibility study, definition of operations and maintenance requirements, functional analysis, concept definition, system maintenance concept, reliability allocation and cost analysis.

Safety is a primary concern for this particular Government organization, as well as any employer, from a total performance perspective, including legal and cost ramifications. An improved safety information system will be more efficient, reducing time spent on paper work, thereby, allowing more time to spent implementing safety controls, saving approximately $978,000 and ultimately yielding a safer, healthier, more productive work environment.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS

CBS	Cost Breakdown Structure
CCB	Configuration Control Board
CD	Collision Detection
CPR	Cardio Pulmonary Resuscitation
CSMA	Carrier Sense Multiple Access
DOS	Disk Operating System
EPA	Environmental Protection Agency
FMEA	Failure Mode and Effect Analysis
GE	General Electric
GEA	General Electric Aerospace
HSRS	Health and Safety Record System
LAN	Local Area Network
M&DSO	Management and Data Systems Operations
MS	Micro Soft
MSCC	Mallinckrodt Specialty Chemical Company
MSDS	Material Safety Data Sheet
MSDSs	Material Safety Data Sheets
MTBF	Mean Time Between Failure
MTBM	Mean Time Between Maintenance
MTTR	Mean Time To Repair
NAF	Nurse Accident Form
NIC	Network Interface Card
OSHA	Occupational Safety and Health Administration
PC	Personal Computer
PCMS	Preventive Maintenance Checks and Services
RAM	Random Access Memory
ROM	Read Only Memory
SMITS	Safety Management Information and Tracking System
TAT	Turn Around Time
UPS	Uninterruptable Power Supply

1.0 EXECUTIVE OVERVIEW

1.1 OBJECTIVE

The objective of this project is to provide a preliminary design for an improved safety information system that will enhance the performance of the Government organization's safety program. The system currently utilized is inefficient, as evidenced by the 1.4 million spent annually on accidents. Much time is spent on paperwork and menial tasks, rather than on safety operations; however, as efficiency of the safety information system increases, more time will be available to perform proactive operations, reducing the number of mishaps, saving money, improving the performance of the safety program and ultimately creating a healthier, safer work environment.

1.2 BACKGROUND

Currently, General Electric Aerospace (GEA) Management and Data Systems Operations (M&DSO) operates the Safety Program at a large Government installation. This installation employs thousands of people who work in offices, laboratories, computer centers, warehouses, construction, ground maintenance, electrical shops, mechanical rooms, and confined spaces throughout the facility. There are numerous chemicals used throughout the facility and employees continually run the risk of exposure. In addition, there are a variety of maintenance activities, building modifications and construction, under ground storage tank work, man-hole issues, building safety concerns, and indoor air quality problems among other issues which require the attention of safety personnel.

The Safety Office has the responsibility of ensuring that the facility maintains a safe and healthy working environment which complies with federal regulations. This charter puts the Safety Office into a service role, responding to and anticipating employee needs and concerns. However, the processes and tools currently used do not promote efficiency.

The GE Safety Office currently consists of 3 employees dedicated full time to safety issues. The Safety Office interfaces regularly with another GE employee responsible for hazardous materials and waste in the logistics branch and a Government employee in the security branch dedicated part time to safety. The Safety Office falls under jurisdiction of the Chief of the Facilities Branch. Figure 1.2-1 illustrates the hierarchy in the chain of command.

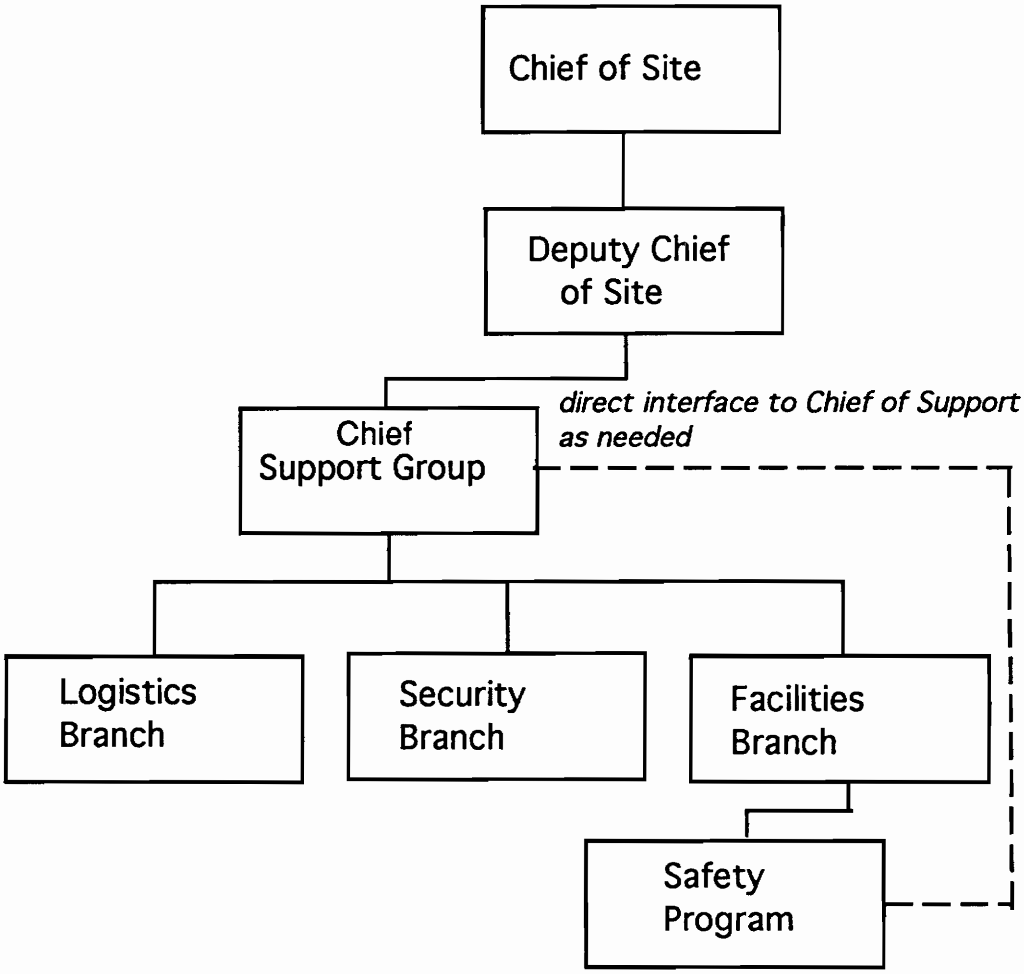


Figure 1.2-1. Government organizational flow.

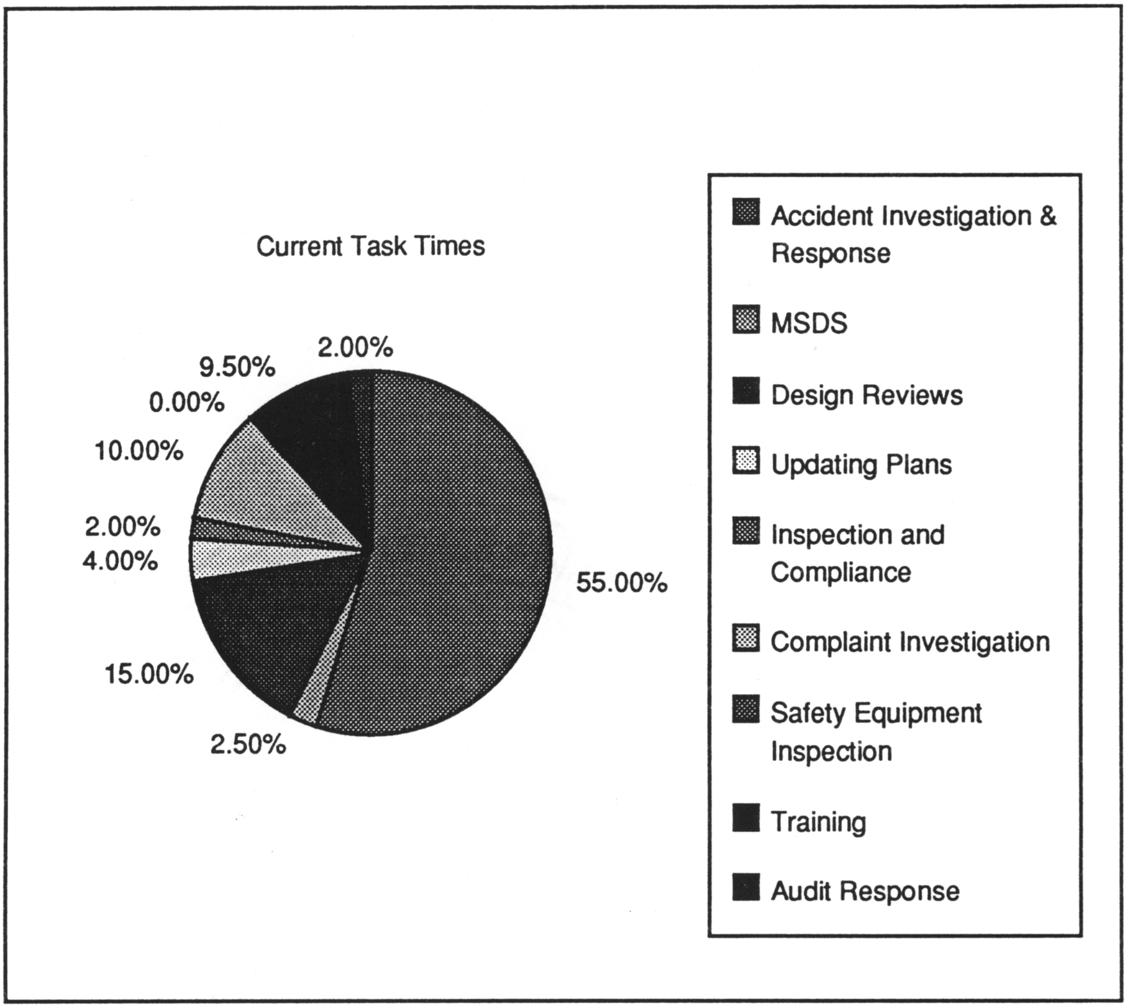
1.3 OUTCOME

The systems engineering methodology is used to obtain a recommended design for a Safety Management Information and Tracking System (SMITS) based on streamlined safety program processes. The SMITS will allow the user to readily access Material Safety Data Sheets (MSDSs), Occupational Safety and Health Administration (OSHA), Environmental Protection Agency (EPA) and Fire and Life Safety Codes, Accident/Incident Forms and statistics and training information. In addition, the system will provide a means for tracking survey status and recommendations and inspection information. This computer system will integrate commercial hardware, commercial software and customized databases to meet the demands of the Government's Safety Program. Because the Safety Program has representatives at satellite locations who require access to the same information, this state of the art system needs to have the *potential* for remote access. Customer demands dictate that this comprehensive safety system be extremely user friendly, easy to maintain and flexible enough to accommodate future requirements.

The outcome of this project is the design for a network configuration of an integrated commercial and custom hardware and software system which provides the user an easy, quick and efficient means of managing a comprehensive safety program.

1.4 BENEFITS

The Safety Program will receive the design for a computer system which facilitates more efficient, productive work processes and a significant cost savings. Figure 1.4-1 compares current task time consumption with anticipated task time consumption after implementation of the SMITS. By decreasing the time spent on paperwork activities the safety program can increase the time spent on safety operations.


Current Task Times
9.50%
2.00%
0.00%
10.00%
2.00%
4.00%
55.00%
15.00%
2.50%
Accident Investigation & Response
MSDS
Design Reviews
Updating Plans
Inspection and Compliance
Complaint Investigation
Safety Equipment Inspection
Training
Audit Response

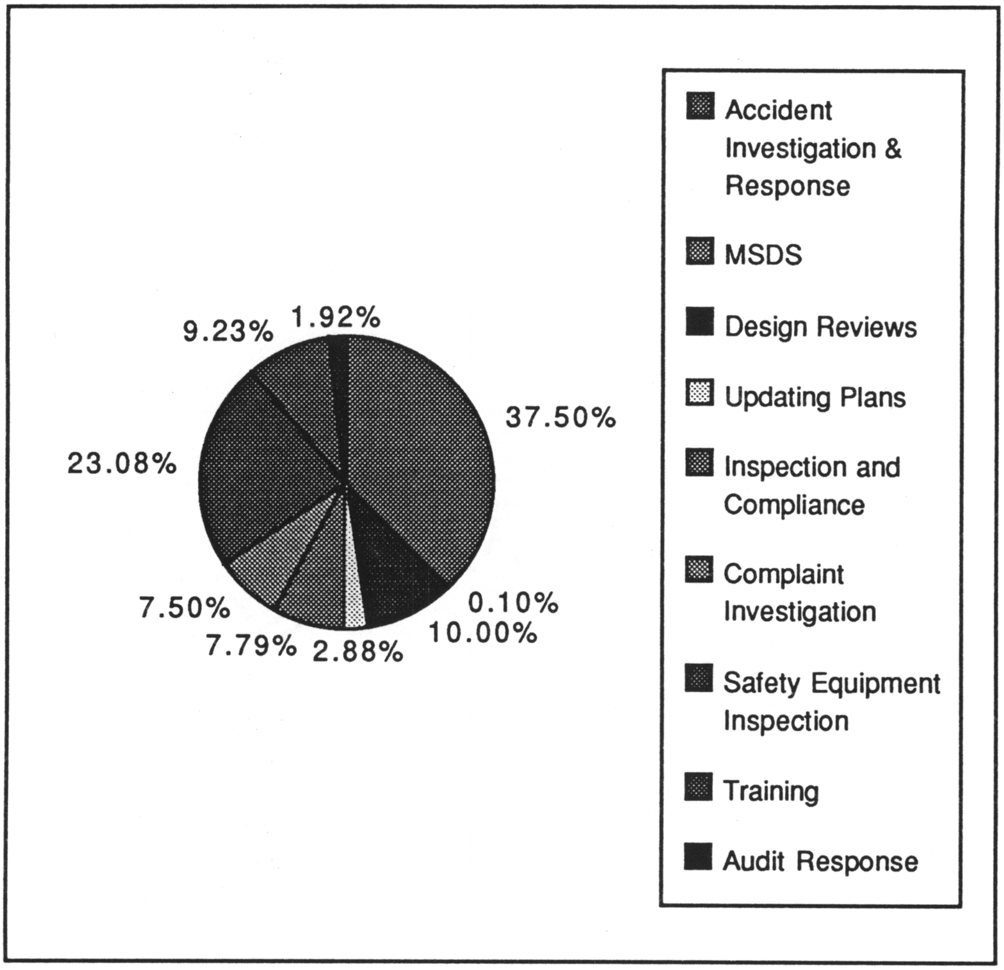


Figure 1.4-1. Task time consumption

Benefits include:

- **Cost savings of 978,000** over operating life cycle;
- Decreased response time in emergency situations requiring immediate access to Material Safety Data Sheets (MSDSs);
- Decreased response time to requests for approval of modifications, renovations and construction;
- Streamlined accident investigation process and simple means of obtaining statistics;

- Means of ensuring that surveys and action items are addressed in a timely manner and recommendations are implemented;
- Means of ensuring that inspections are conducted in a timely manner and equipment is not misplaced;
- Increased efficiency and productivity of the Safety Office;
- Streamlined processes;
- Ultimately, a safer, healthier work environment.

1.5 METHODOLOGY

In order to design the SMITS, the systems engineering process outlined in Blanchard and Fabrycky's Systems Engineering and Analysis text is followed. Figure 1.5-1 adapted and modified from the text shows the portion of the systems life-cycle process applied in this paper. Implementation of the proposed SMITS will result in design, development and operations occurring in accordance with Blanchard's life cycle process flow.[1]

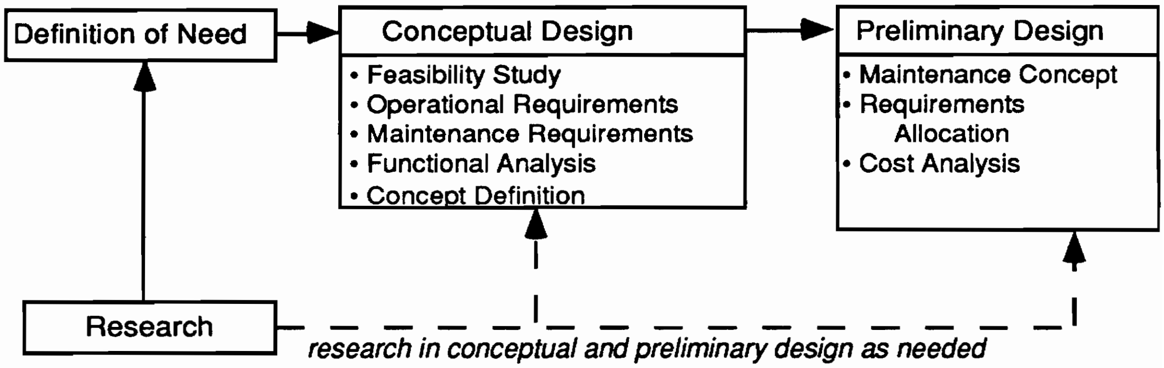


Figure 1.5-1. Systems life cycle process tailored for SMITS.[2]

First the definition of need is established. The Conceptual Design follows, encompassing feasibility and requirements. The feasibility study is conducted addressing potential solutions and SMITS operational and

---

[1] Benjamin Blanchard and Wolter Fabrycky. *Systems Engineering and Analysis* (Englewood Cliffs: Prentice Hall, 1990) p. 22.

[2] Blanchard p 22.

maintenance requirements are defined. Throughout this process there was significant interaction with the customer (the Safety Program staff and interfaces) to identify and prioritize needs. In addition, resources and experts were consulted to determine the feasibility of SMITS requirements and potential for applications in other arenas. The functional analysis follows the requirements definition. The Conceptual Design phase terminates with the SMITS concept definition.

The Preliminary Design of SMITS follows the Conceptual Design. The Maintenance Concept is proposed. Performance, design and effectiveness factors are allocated along with system support requirements. A life cycle cost analysis follows allocation.

1.6 RESOURCES UTILIZED

In order to ensure that the optimum design configuration was attained, various resources were utilized. These included: safety experts and salespeople, computer books, computer experts, computer salespeople, software experts, software literature, companies with existing safety systems and the customer. References are contained in Section 11.

2.0 DEFINITION OF NEED

2.1 BACKGROUND

The Safety Program at a rather large military facility, herein identified as the Government, is run by General Electric (GE) Management and Data Systems Operations (M&DSO) representatives. There are numerous types of activities conducted at the Government site and safety is a prime concern (see Section 1.2 for more detail). Current safety practices tend to be reactive rather than proactive because the Safety Staff is so busy "putting out fires"[1]. The employees are indisputably experts in their fields and respected for their contributions, but their processes, tools and mode of operation do not foster efficiency.

As a temporary safety engineer in the user environment it became apparent that a study of the users' roles, responsibilities, and internal and external customers was needed. This opportunity provided first hand knowledge and understanding of the operating environment and the nature of the deficiency.

The Safety Office has a plethora of responsibilities, including:

- responding to and investigating accidents,
- maintaining current chemical inventory of buildings and Material Safety Data Sheets (MSDSs),
- ensuring proper storage, handling and disposal of hazardous materials and waste,
- participating in design reviews of new systems, facility modifications and facility construction,
- updating emergency evacuation plans and procedures,
- inspecting buildings and providing recommendations to improve, correct or eliminate deficiencies,
- ensuring compliance with Occupational Safety and Health Administration (OSHA) and Environmental Protection Agency (EPA) codes and regulations,

---

[1] David Nay, Safety Engineer, General Electric, interview, Springfield, Virginia, 25 February 1993.

- inspecting safety equipment (fire extinguishers, eye wash stations, emergency showers),
- investigating any building resident complaint, such as odors, heat, air quality, potential safety hazards, ergonomics,
- training new employees on Safety,
- training all building residents in OSHA Right To Know classes,
- providing training for special task teams as required, such as asbestos removal, respirator certification, Cardio Pulmonary Resuscitation (CPR), Fire and Life Safety, and
- responding to EPA and OSHA audits.

However, the processes and tools used to perform these tasks (explained in the ensuing sections) inhibit the efficiency of the Safety Program. As a result, the Safety Program tends to be reactive, and a truly efficient and effective safety program needs to be proactive - building controls into the facility to prevent incidents rather than responding to mishap. Figure 1.4-1 illustrates the percentage of time currently expended on Safety Program tasks. Reducing the amount of time spent on these tasks through more efficient processes will allow more time to be dedicated to instituting proactive safety controls, preventing mishap and thus freeing even more time to implement safety controls. It is estimated that 978,000 dollars will be saved over the SMITS operating life time as a result of a decrease in the number of accidents alone. This does not include potential savings associated with preventing a OSHA or EPA fine, which vary in cost depending upon the severity but can be thousands of dollars, or the costs associated with chemical spill response, and fire prevention/reaction among others.

2.2 OVERVIEW OF SAFETY MANAGEMENT PROGRAM

This section describes the current *modus operandi* for safety program tasks so that when the user deficiency is defined, it is understandable.

2.2.1 Accident Investigation and Reporting

Figure 2.2.1-1 outlines the process flow for accidents occurring at the Government site.

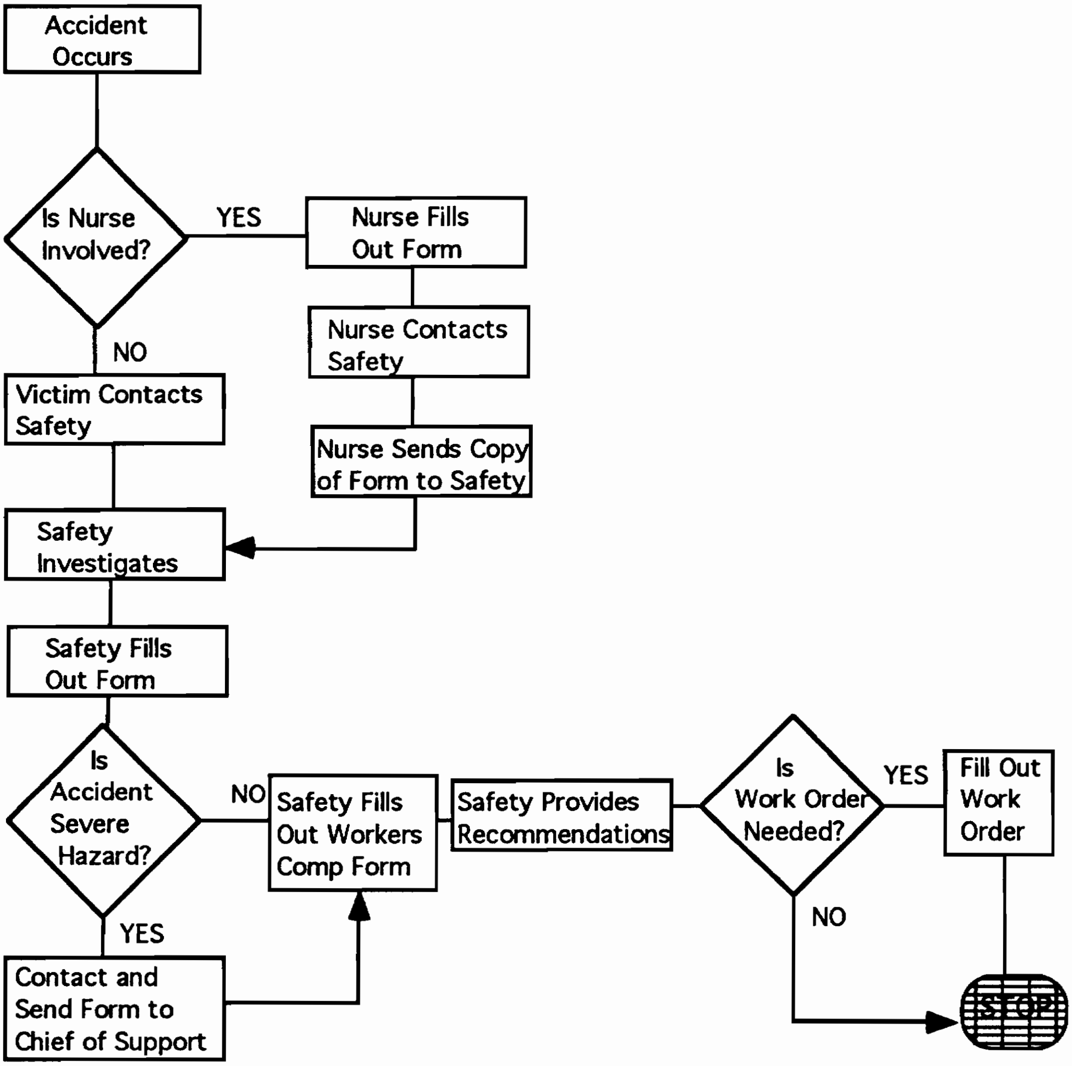


Figure 2.2.1-1. Accident Investigation and Reporting Process.

If the nurse is involved, she fills out a form regarding the accident, employee identification and treatment, calls the Safety Office to notify them of the problem, and sends the Safety Office a copy of the form. The Safety Office, notified of the accident by either the nurse or the individual investigates the accident by interviewing the victim and examining the area in which the accident occurred. Safety then completes the form contained in Appendix A and the workers compensation form also contained in Appendix A.

If Safety determines that there is something in the work environment which can be changed to prevent recurrence of the accident, Safety provides recommendations to implement these changes. If the change requires modifications or expertise to implement, Safety writes a work order request. If it is the end of the month, safety compiles the monthly statistics as required by upper management. At the end of the year, Safety completes the form contained in Appendix A as mandated by OSHA. It is estimated that up to 15 accidents may occur each week each requiring up to 2.5 hours to investigate and document.

2.2.2 MSDS and OSHA/EPA Regulations

Currently, the Safety Office and the Logistics Branch maintain complete volumes of MSDSs. When products are received, the MSDS is distributed to the Logistics Officer who numbers the MSDS, copies the MSDS and sends the copy to Safety. The Logistics Officer maintains a list of products, by number, on a computer. Every time a new product is ordered, it is assigned a new number; numbers associated with products which are not ordered anymore are reassigned as the product is removed from the facility.

However, this is the "ideal" process. In actuality, the Safety Office falls behind on the clerical task of replacing old MSDSs with new MSDSs and often stacks of MSDSs accumulate. Other times, MSDSs are filed inappropriately. Another problem with this process is the products are arranged on a random number scheme; when a chemical spills it is difficult to locate the MSDS since they are organized numerically on both the chemical list and in the MSDS volumes. Additionally, each area on the installation is supposed to have a complete, updated binder containing MSDSs for the chemicals used in that area. There is no mechanism or process in place at this time to distribute MSDSs to these areas.

Similarly, EPA and OSHA regulations are kept in various locations throughout the Safety Office. When needed, employees can reference the manuals; however, accessing information within the manuals is tedious and time consuming as it is often difficult to locate the relevant text because of the manuals' organization. Thus, the safety officer is spending valuable time performing a retrieval task instead of implementing safety controls.

2.2.3 Surveys and Inspections

The Safety Program is under contract to conduct surveys and inspections on a "regular" basis to ensure that the facility complies with OSHA and EPA regulations and that safe work practices are employed. The Safety Officer will investigate the area using an inspection checklist. Following the survey, the Safety Officer documents the results and recommendations, briefs management, and writes work orders to implement approved recommendations. Once the work order is completed, there is no routine follow-up to ensure that the work was conducted or that the recommendation was correctly implemented. Unfortunately, the Safety Program is so busy responding to employee complaints, concerns and requirements that surveys and inspections are not conducted as "regularly" as they should be. It is rare that the Safety Program manages to spend more than one week for site inspections

In addition to inspecting facilities, the Safety Program is tasked with ensuring that fire extinguishers, emergency eyewashes and safety showers are functional. OSHA requires fire extinguisher inspection monthly; this entails ensuring that the extinguisher is not discharged, the pin is in place, the nozzle is free from obstruction and that the position of the extinguisher is within OSHA requirements as depicted in figure 2.2.3-1.

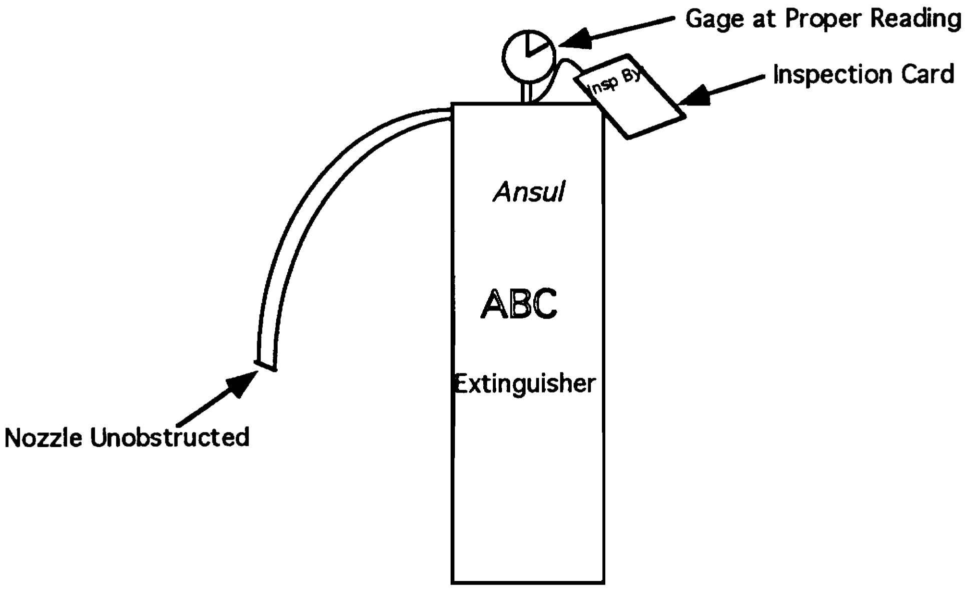


Figure 2.2.3-1. Fire extinguisher inspection.

At this time, fire extinguishers are not routinely inspected and replacements or recharging occur only when brought to the attention of the Safety Program. This reactive response runs the risk of a fire occurring and no fire extinguisher being readily available to extinguish it. There is no quantifiable measure to evaluate the cost of inspection versus the cost of lives.

2.2.4 Training

The Safety Program tasks include providing training for employees as required by federal regulations. For example, all employees are supposed to receive Hazardous Communication training and emergency evacuation training. Other employees require, for example, driver certification, asbestos removal certification, hazardous materials handling training and incident response certification. Safety accomplishes training by either conducting courses in-house themselves, contracting a consultant to train on-site, or sending employees to a training course. The record keeping of who attended classes and who requires training is not centralized so often the Safety Office is negligent in identifying participant training requirements in a timely manner. In addition, outside training courses involve resources, signatures, input and logistics support from other branches. This part of the process, which occurs outside the realm of the Safety Program, is cumbersome and often hinders timely training.

2.3 NATURE OF DEFICIENCY

Currently, approximately 462 accidents occur per year, resulting in a cost to the Government of $1.4 million.[1] This is nothing but a waste of money - it is not being re-invested, it will not result in improved performance, it is simply lost money. The number of accidents is so high because the Safety Program does not have enough time to implement proactive measures such as surveying and inspecting the facility. Rather, the Safety Program time is spent inefficiently on processes and procedures which are tedious, time consuming and redundant. Table 2.3-1 compares the amount of time spent now on tasks and the amount of time which could be spent on tasks after implementation of an improved safety information system. Increasing time spent on inspections and fire and life safety equipment inspections is good, as these are proactive tasks which help reduce personnel and facility risk.

---

[1] Nay.

Table 2.3-1. Safety task times.

PRIMARY SAFETY TASKS	TIME SPENT PER YEAR NOW (hrs)	PERCENT NOW	TIME SPENT PER YEAR POST SMITS	PERCENT POST SMITS	TIME DELTA POST SMITS (hrs)
Accident Investigation & Response	1156	55	780	37.5	-376
MSDS	52	2.5	2	0	-50
Design Reviews	312	15	208	10	-104
Updating Plans	80	4	60	3	-20
Inspection and Compliance	40	2	162	8	122
Complaint Investigation	208	10	156	7	-52
Safety Equipment Inspection	0	0	480	23	480
Training	192	9.5	192	9.5	0
Audit Response	40	2	40	2	0
TOTAL	2080	100	2080	100	

Material Safety Data Sheets (MSDSs), Occupational Safety and Health Act (OSHA) and Environmental Protection Agency (EPA) regulations, Fire and Life Safety Codes, Accident/Incident Investigation Forms and Training Documentation are stored haphazardly and incompletely throughout various offices. Inspections of safety equipment, such as fire extinguishers and emergency eye wash stations are not documented and often not conducted. In addition, survey recommendations and corrective actions are not tracked, and as a result are often neglected. When information needs to be accessed, employees have to search a variety of sources and locations. Furthermore, there are no tools or processes in place to facilitate the job of the Safety Office, to assist with new employees coming up to speed or to ensure that the site personnel demands are satisfied.

For example, the Safety Program currently fills out 2 different forms every time there is an incident or an accident - one for Workman's Compensation, one for the Safety Office and one for the Government in addition to a form filled out by the Nurse. Not only is this process of 3 forms with similar information redundant, but the manual storage and retrieval of this information is cumbersome. These forms are used to measure productivity and determine statistics monthly and the data is used to report to OSHA as mandated by the Occupational Safety and Health Act of 1970. In order to tabulate accident and incident rates, the files must be sorted through manually and the statistics obtained.

Additionally, a more timely response is needed from the Safety Office in the event of a chemical spill. In this type of emergency, the MSDS needs to be referenced to obtain information on how to clean up the spill, what protective equipment to wear and what authorities to notify. Reaction time is critical. Yet to obtain an MSDS under the current manual configuration, the MSDS binders must be searched. While the search for the necessary information is in process, a dangerous chemical may be leaking into a sewer, the ground or an office or severely injuring an employee.

During construction and renovation, the Safety Office is responsible for ensuring that the structure is safe and compliant with the intent of the OSHA, EPA and Fire and Life Safety Regulations. Means of egress usually plays a significant role in the Safety Office evaluation. To determine safe egress, many different OSHA and Fire and Life Safety volumes need to be consulted - to classify the area and to determine if requirements are satisfied. This process can take as long as three hours as an employee flips through various references.

Surveys and inspections are conducted in a reactive rather than proactive mode. OSHA regulations require fire extinguishers to be inspected every 30 days and yet many extinguishers are not even checked yearly. A recent site survey indicated that 54% of site fire extinguishers have not been inspected within the last 12 months.[1] This is because the extinguisher existence is unknown and poor preventive maintenance processes.

Building surveys identify potential hazards and code deficiencies; however, poor follow up leads to many recommendations falling by the wayside, the result being an accident which could have been prevented had the recommendation been implemented. Recently, a political fiasco resulted when it was discovered that recommendations from one year

---

[1] Nay.

ago were not yet implemented because they had been "lost" - fortunately, no one was hurt during the time the recommendations were in limbo.

Streamlining existing processes will improve the efficiency and productivity of the Safety Program, allowing more time to be spent on important safety tasks rather than on information hunting and gathering and report generation. As a result, the number of accidents will decrease and less money will be spent on worker's compensation and lost time. Improved efficiency will improve the performance of the Safety Program, resulting in less mishap and a safer, healthier work environment at the Government site.

2.4 STATEMENT OF NEED

The current non-streamlined, non-automated processes are costly, inefficient and potentially dangerous. These processes are costly because the large number of accidents per year results in a cost of approximately 1.4 million dollars. The inefficiency of the processes stems from the excessive amount of time spent on tasks (see figure 1.4-1). The processes are potentially dangerous because fire and life safety equipment is not properly maintained nor are building surveys and inspections corrected regularly.

The Safety Program requires a safety system which will facilitate job performance, thereby decreasing inefficiency, reducing costs and decreasing the annual accident rate. The Safety Program employees are currently not computer proficient, so a computerized solution must be extremely easy to use. It is imperative that the safety officers do not suffer from "information anxiety... which results when you know what you want, but not how to get it" as defined by Saul Wurman in his book Information Anxiety. Besides being *user harmonious*, the system must be responsive. If the system is so slow that the user could have accessed the information quicker sorting through information using the current process, the user will not continue to use the system. The system must be easy to maintain, have technical support available on an as needed basis and come with training courses and documentation. The system must be designed ergonomically to optimize the user-system interface.

Furthermore, the system must be designed with the potential for future upgrades and enhancements. The system must have the potential to accommodate users at different Government sites. Table 2.4-1 summarizes the user performance characteristics.

Table 2.4-1. Summary of User Performance Characteristics.

User Needs
Facilitate Job Performance
User Harmonious
Responsive
Maintainable
Technical Support Available
Training
Documentation
Ergonomic
Enhancement/Upgrade Potential
Potential for Multiple Locations

2.5 OPERATIONAL NEED

Future down-sizing plans impact the Safety Office staff. The Safety Program Office direct staff will be cut by 33% by 31 December 1995; however, current job responsibilities will grow as the Government becomes more environmentally conscious and federal facilities lose exemption to EPA and OSHA regulations. As a result it is extremely imperative that the efficiency and productivity of the office improve so that performance does not suffer as a result of the down-sizing. In addition, if attrition occurs with the experienced safety personnel, finding and training replacements will be extremely challenging as there is no established in-house safety officer training program.

An improved safety management process and tracking system will improve Safety Program efficiency and thus performance, and is required to be operational by the end of December 1993 to ensure smooth transition between the down-sizing and the system installation and usage.

2.6 RESOURCES

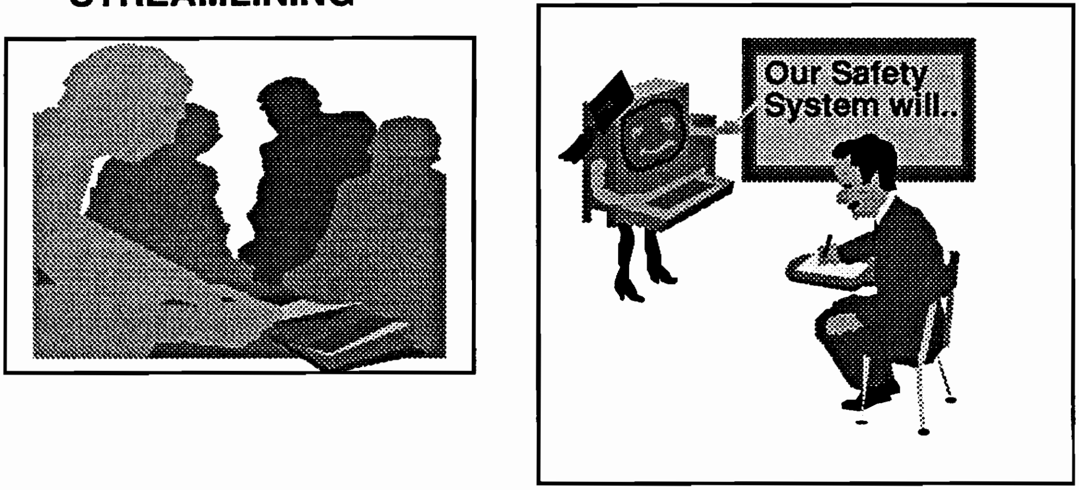
Because of the shrinking defense budget and the emphasis on competitiveness, overhead money is scarce. However, $100,000 has been budgeted for improving the Safety Office. Although the Government mandated staff reductions across all disciplines at the site, liability for the remaining approximate 1700 workers is a prime concern.

To improve efficiency of the Safety Program while at a minimum maintaining performance with a reduced staff requires improved processes, tools and techniques. The Government recognizes this and consequently places this system in a high priority category, and has allocated money and personnel to acquire the system.

3.0 FEASIBILITY STUDY

3.1 INTRODUCTION

The purpose of the feasibility study is to identify technology approaches which may satisfy the user requirements. For the SMITS, a few options exist, such as: streamlining existing processes, using an existing safety system, and automating the Safety Office. These choices are depicted in figure 3.1-1 and described in the following sections.



STREAMLINING

EXISTING SAFETY SYSTEM

AUTOMATION

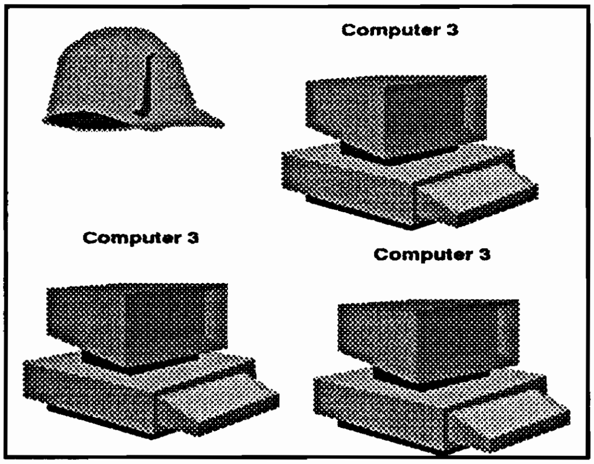


Figure 3.1-1. Potential SMITS solutions.

3.2 WORK SIMPLIFICATION

An information system is any method by which you obtain information, informally or formally - an individual who obtains information from co-workers has set up an "information system", a boss who walks the floor every afternoon to talk to workers is using an "information system", a computer whiz who relies on a baseball statistics model to predict games has established an "information system". The current system in the Safety Office is an "information system" - searching for files, groping for answers, hunting for reports - it is just not the most efficient information system.

An efficient information system facilitates the flow of information, eliminating unnecessary process steps and delays - streamlining the process, just as a production process may be streamlined by re-locating machines to reduce transportation time. Work simplification is the "organization of applied common sense"[1] - allowing the people who do the work to apply easy to understand tools, such as process charting, to improve performance. The Safety Program processes, such as accident/incident investigation and reporting, could benefit from work simplification. There are five steps to work simplification:

1. Select a job to improve;
2. Gather all of the facts and develop a process chart;
3. Challenge *every* detail, asking:
    What, and Why?
    Where, and Why?
    When, and Why?
    Who, and Why?
    How, and Why?

with the focus of trying to eliminate, combine or change.

4. Develop a preferred method;
5. Install preferred method and measure results.[2]

---

[1] Ben S. Graham, Jr., "Work Simplification: From Bricklayer to Microcomputer," *Templates For Information Resources Management*, p. 10.

[2] Allan Mogensen, "Work Simplification - A Program of Continuous Improvement", *Industrial Engineering Handbook*, p. 10-83 through 10-191.

Work simplification techniques have been successfully employed in many applications - from manufacturing to paper (*paperwork simplification*) processes. Gerald Deighton applied work simplification to paper processes at the Federal Drug Administration (FDA) and found the process "sensible...the tools and techniques are easy to learn, do not require a significant learning curve and are applicable to all aspects of business. The process involves continually challenging existing methods, always striving to improve".[1]

Applying work simplification to the existing safety information system potentially offers an improvement to the user's current system Streamlining would include training Safety Program employees on work simplification fundamentals and information process charting and providing a means for the employees to gather together to challenge existing processes. Some Safety Program tasks where work simplification could be applied include:

- Storage and retrieval of all reference books,
- Accident/Incident Investigation process,
- Organizational and reporting structure of the Safety Program,
- MSDSs and chemical inventory process,
- Survey and inspection documentation, and
- Training requirements, selection and documentation.

Applying work simplification techniques to the Safety Program processes is an inexpensive means to improve performance. Too often people become caught in the paradigm of doing things a certain way because that's the way they've always been done. By applying work simplification techniques, Safety Program employees can constructively challenge the existing system and adopt a more efficient means of performing.

While streamlining processes and procedures is an inexpensive solution to help the Safety Program, it does not necessarily eliminate the problems associated with time critical response, inspecting emergency

---

[1] Gerald Deighton, telephone interview on paperwork simplification at the FDA, 29 March 1993.

eye washes, fire extinguishers and safety showers, or knowing where to search to find the right information. These deficiencies would still exist, even though the Safety Program processes would be better organized.

3.3 EXISTING SAFETY SYSTEM

The corporate and global emphasis on EHS issues and moral responsibility to cope with the social and financial impacts of these issues, as well as the introduction of OSHA's new process safety management standard has led many companies, such as GE Aerospace (GEA), the Department of Defense and Mallinckrodt Specialty Chemicals Company (MSCC) to implement their own safety systems.

3.3.1 General Electric Aerospace Safety System

GE Aerospace currently has an automated information system for Safety, the Health and Safety Record System (HSRS). HSRS users span Utica, Binghamton, Syracuse, Valley Forge, Camden, Moorestown, and Pittsfield. HSRS was strategically developed for all of GE Aerospace and resides on an IBM mainframe in Cincinnati, Ohio. The system allows users to access MSDSs, track training, maintain toxicology and exposure data and automate OSHA record keeping. The system also provides for accident investigation.

Discussion with HSRS users revealed that the system is not considered user friendly. The system was implemented over 10 years, and the software and user interfaces have not been updated to reflect current technology. Furthermore, the system capabilities are generic and do not meet individual program requirements. For example, because workman's compensation requirements vary from state-to-state, the accident investigation forms are generic and often "more trouble than they are worth"[1]. Safety concerns at a plant manufacturing satellites are different than those at chemical lab. In addition, every MSDS had to be keypunched into the system in a special format prior to the system going operational which was "a real pain...now it is not so much of a hassle

---

[1] Charlie Chilton, telephone interview on HSRS, 25 February 1993.

because most of the MSDSs are on the system and it's only ones and twosies that need to be keypunched."[1] Additionally, the system is "as reliable as the people who put the information onto it"[2].

It would be fairly easy for GE M&DSO in the Washington Area to link into the HSRS; however, this would not satisfy the demands of the Government. The system does not meet all of the user's requirements, and:

- GE would not allow a Customer to use a proprietary system because the system was developed by GE for GEA facilities using GEA overhead funds and there would be no benefit to let an outsider use the system; it would be the same as Nabisco letting Pepperidge Farm use it's ovens;
- Government security would not allow a connection from the Customer site do a GE facility;
- Customer chemical inventory and MSDSs are considered sensitive and could not be placed on an open system.

However, establishing an HSRS connection at Washington is an idea worth exploring for the GE in the Washington Area.

3.3.2 Department of Defense

Another safety information system currently used in the Department of Defense relies primarily on the manual search, sort and hunt similar to the method used at the Government in conjunction with some automation. The Department of Defense has various buildings and each has a designated safety officer responsible for implementing their own processes and procedures for complying with federal, state and local laws as well as maintaining a safe and healthy work place.

Accident investigations and statistics were automated at one time at the Department of Defense headquarters; however, the maintenance of the system fell by the wayside as no one wanted to enter the data onto the computer and the information provided was not very valuable. The information was broken up into too much detail (i.e. slips on stairs, slips

---

[1] Chilton.

[2] Chuck Fazio, telephone interview, 26 February 1993.

in cafeteria, minor burns, major burns, bumps, etc.) so that when the matrix was developed each year showing accident statistics, trends were not apparent. The system did indicate if certain locations suffered more accidents than another location; however, the difficulty associated with entering information was not worth the output. Material Safety Data Sheets are maintained in hard copy, thus, maintenance is difficult. Inspections and surveys are conducted at each site by the resident safety officer. Training records are maintained manually by the headquarters safety office. The chief of the safety office did not see a need for a computer system for the Department of Defense since it was "mostly paper oriented" and the computer was really "a status symbol" but admitted he "was not a computer buff".[1] Based on the conversation, it seems that this could be a potential market for an improved system similar to the HSRS.

3.3.3 Mallinckrodt Specialty Chemicals Company

The Safety Management Newsletter identified Mallinckrodt Specialty Chemicals Company (MSCC) as a leader in compliance with OSHA's Process Safety Management Standard. Dale J. Schillinger MSCC's director of safety and health identified seven rules for safety:

- A system to verify that changes don't threaten safety;
- Pre-start up reviews;
- Process audits;
- Accident investigations;
- Emergency plans;
- Training verifications for contractors; and
- Employee training.

Each of MSCC's sites is responsible for compliance. The system focuses on building safety backups into designs up front, reviewing processes in a class room atmosphere, analyzing the impact of variable changes and walking through plants to highlight safety problems. Accidents are investigated and corrective action taken to prevent recurrence. Training

---

[1] Bill Macher, telephone interview, Washington D.C., March 1993.

information is maintained in a database system. The entire system is not automated and sites can not electronically communicate and Mr. Schillinger doesn't see "a need for automation nor have time to use automation at MSCC headquarters"[1] although each MSCC site has automated portions of it's safety program, such as training data.

3.3.4 Lessons Learned

The importance of including the user in the requirements definition phase is apparent based on interviews with the safety representatives from GE and Department of Defense. Had the users been more involved with the system development, the delivered systems would have satisfied their requirements. Additionally, including the user in the system development process ensures that the user is *buying into* the concept. The safety representatives interviewed were skeptical and hesitant about automation - and the two companies with the automated systems did not use them. Knowing this prejudice exists prior to implementing a system will help the system designer and developer overcome the bias.

3.4 AUTOMATION

The prevalence of computers and computer products throughout business, home, and schools is indicative of both the availability of and dependence on computer systems and automation. In the past decade, technological advancements and competition have driven computer prices to an affordable level while performance has increased significantly. Computer technology is available - the difficulty resides in making educated, informed decisions regarding hardware and software selections.

For the SMITS, there are many options and potential configurations which will satisfy the user's need. The challenge is to develop a system that meets the user's need and will continue to meet the users' needs in the future without over designing - there is no reason to design a Mercedes when a Honda will satisfy the requirements. This

---

[1] Dale J. Schillinger, telephone interview, March 1993.

is especially difficult when confronted with the plethora of hardware and software currently available. In addition, the system needs to reduce the amount of work of a safety program. Finally, there is the negative stigma associated with information systems to overcome - interviews with three corporate safety offices indicated skepticism relating to information systems.

Because there are a few SMITS users requiring access to the same information, it is most likely that some type of connectivity among the computers is needed, if automation is indeed a "requirement". The size of the system and the type of system will be driven by the requirements of the selected software and external interface requirements. Connectivity and networks are addressed in Section 3.4.1.

Bar coding is a potential solution for the user's fire extinguisher, safety shower and emergency eyewash inspection requirement. This is addressed in Section 3.4.2

3.4.1 Networks and Local Area Networks

There are different methods for connecting personal computers (PCs), depending upon the complexity of the user's needs, including:

- Simple printer sharing and file transfer;
- 2-20 PCs in a local area network configuration
- 20-200 or more nodes with multiple servers;
- Interoperability.

Simple printer sharing and file transfer is appropriate for an environment where users share the same printer and desire to share files without having to transfer diskettes. Networks are used for more than one user when high speed information sharing is necessary. A full time person is not needed to manage this type of network, rather a part time Local Area Network (LAN) caretaker is recommended to look after the system. Systems requiring a large number of nodes or workstations usually require the help of computer integrators and installers. Interoperability refers to users who need to integrate many networks from various vendors.[1] The SMITS user profile most closely mirrors the 2-20 PCs in a local network configuration.

A Local Area Network (LAN) is a "...communications network that provides interconnection of a variety of data communicating devices within a small area"[2]. A small area is limited to a building or occasionally several buildings on the same compound in a mile radius; for the SMITS customer it is confined to one office area. LAN communication speeds are usually quick and the error rate is relatively low because the LAN does not span a large geographical area. Table 3.4-1 contains the characteristics typical of LANs.

Table 3.4-1. LAN characteristics

Low Error Rate	10^{-8} to 10^{-11}
Short Distances	.1 to 25 km
High Data Rates	.1 to 100 Mbps

LANs have been available since the early seventies when they emerged as an alternative to mainframes.[3] Because the technology has been implemented for more than twenty years it is proven and available. Competition, performance improvement and advancements in architecture and execution networking software have significantly improved features available from current LAN systems.

Figure 3.4.1-1 illustrates a basic LAN configuration.

---

[1] Frank J. Derfler. *Guide to Connectivity* (Emeryville, CA: Ziff-Davis Press, 1992), p. 5-7.

[2] William Stallings, *Local Networks* (New York: Macmillan Publishing Company, 1990), p. 2.

[3] Abraham Silberschatz, et al., *Operating System Concepts* (New York: Addison-Welsley Publishing Company, 1991), p. 448-449.

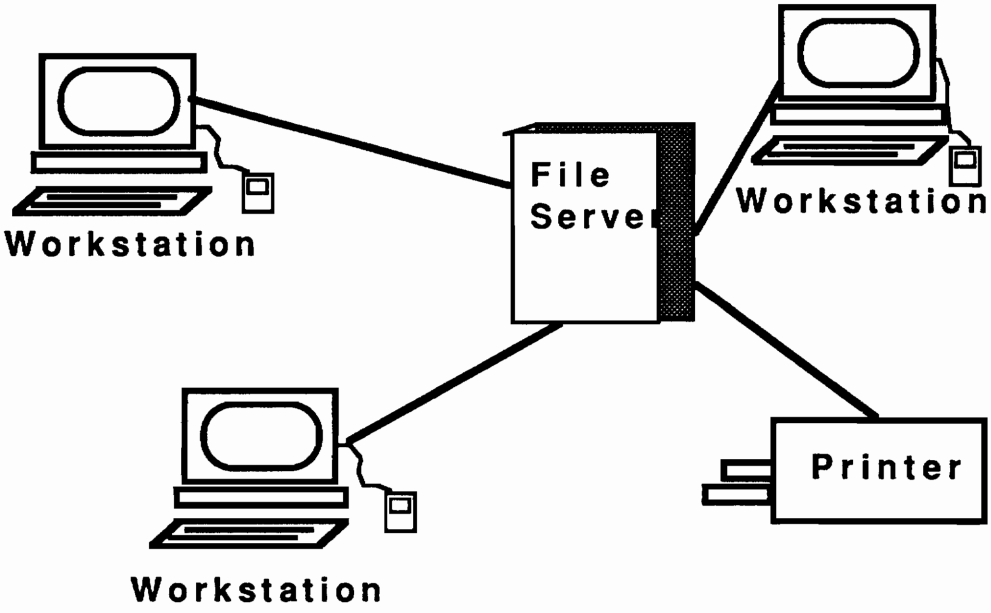


Figure 3.4.1-1. Typical LAN configuration

LANs may consist of PCs acting as *servers* and PCs acting as *clients*. The server is the device which shares it's resources over the network. There are three types of servers:

- *file servers*, which store files for client computers while software in the client PC makes the file servers' hard disks and/or CD-ROM drives appear to be local drives on the client computers;
- *print servers*, which provide the capability of sharing a printer across the network, and
- *communication servers*, which make off-LAN communications links (i.e. LAN to LAN connection) available to clients

Often the server is separate from the client as is the case of the *client/server* model which requires that one computer be dedicated as the file server. The *peer-to-peer* configuration allows any PC on the network to function as both the workstation and the server.

Because there are so many configuration, medium, hardware and software options, there are many potential systems which could be used for SMITS. For example, the SMITS could use:

a) a Macintosh hardware platform, running under Apple Talk which allows users to share files and printers.

b) a SUN System based under a UNIX operating system such as Banyan's VINES or Novell's Netware.

c) an IBM PC or compatible system running under MS DOS and networked with Ethernet LAN adapter cards and Novell software (Novell modifies DOS so that user stations have client and server capabilities).

d) an IBM PC or compatible system sharing files and printers using Windows for Workgroups which sets up peer-to-peer type of configuration.

3.4.2 Software

Various software packages exist which could meet user needs. Databases could be developed using a commercially available package such as Paradox or MS Access to support the accident investigation and reporting process, to facilitate training, to track surveys and inspections and the resulting recommendations and to maintain the chemical inventory. Or, similar solutions could be achieved using a spreadsheet, such as Quatro Pro, Lotus 123 or MS Excel. In addition, there are some commercially available packages which are available through the National Safety Council to facilitate accident record keeping, to maintain chemical inventories and to provide guidelines in emergency response situations. Software for an automated solution to the user deficiency is plentiful.

3.4.3 Hardware, Software Summary

There are several types of hardware and software platforms available for LAN configuration and various vendors for both hardware and software; certain software and hardware decisions impact and often dictate other software and hardware selections and configurations.

These options and their trade-offs are addressed in Section 5.0, Design Concept. The important concept is that computers and connectivity are readily available and sufficiently robust to support user requirements.

3.4.4 Bar Coding

Bar coding provides a cost effective, accurate, efficient means for systematically collecting and identifying data collection. Bar coding technology is used commonly - from grocery and department stores to postal services. There are several companies which provide bar coding systems which are portable and can be used for inventory control, which is pertinent to the user's need for inspection and maintenance of fire extinguishers and other safety devices.

Bar coding systems require labels, which can be printed in-house or purchased from an outside vendor. The labels contain the bar code and are placed on the items being coded. In addition, bar coding systems have a reading device or scanner - either contact or non-contact. Contact units must either physically touch or come in close proximity to the bar code and are typically hand-held; non-contact units are either stationary or hand-held and do not have to come in contact with the bar code symbol. After a symbol is read, the information can be stored for later use, transmitted to a host computer or used immediately in conjunction with information stored in the memory.

OSHA requirements dictate that fire extinguishers, safety showers and emergency eye washes be inspected every 30 days. The Government site contains approximately 1245 of these items. The site consists of several buildings and the safety devices are dispersed throughout all of the buildings and parking lots. It is estimated that an individual inspector would require a minimum of two 40 hours work weeks to conduct a comprehensive inspection, which implies that 50% of this individual's job would consist of inspections. It is estimated that with a bar code system the inspections would be reduced to a maximum of one 40 hour work week.

At this time, there is no established periodic maintenance and inspection of these devices because support is not available. Bar coding technology is a viable means of inspecting and tracking fire extinguishers, safety showers and emergency eye washes. In addition to bar coding companies which sell components individually, there are vendors with systems already designed specifically for safety applications, referred to as "turn-key systems".

3.5 Conclusion

Using the information discovered during the feasibility study as lessons learned in conjunction with the requirements will lead to a recommended solution for SMITS. Based on the feasibility study alone, work simplification should be used to streamline current Safety Office processes, such as accident investigation and reporting - it is cheap and effective. If automation remains a viable solution after requirements are defined, streamlining should be conducted *prior* to automating the system to improve the efficiency of the automated SMITS. Heeding the complaints expressed by users of existing systems will enable the SMITS to avoid the same pitfalls. Using this information, an optimum information system can be designed . Section 5.0 contains the functional analysis and section 6.0 addresses the design concept and trade-offs.

4.0 REQUIREMENTS

4.1 MISSION DEFINITION

The primary operating function of the system is to facilitate the tasks of the Safety Officer. The system shall accomplish this by:

- Providing Material Safety Data Sheets (MSDS) in a data store and retrieve mode that is easily accessible to the user
- Providing current Environmental Protection Agency (EPA) and Occupational Safety and Health Act (OSHA) regulations in a data store and retrieve mode that is easily accessible to the user
- Streamlining accident investigation reporting and statistical measuring methods
- Tracking employee EHS training requirements and courses attended
- Tracking fire extinguisher, emergency eyewash and shower inspections and locations
- Tracking building survey/inspections and resulting recommendations
- Standardizing and centralizing the site chemical inventory
- Providing report and presentation generation and writing techniques using information entered by the user as well as information obtained from other functions (i.e. accident investigation output)

A secondary mission of the system is to provide users with a word processing and presentation platform. The system will accomplish it's objectives by automating Safety Program practices. This automation will consist of hardware and software platforms interacting to meet the requirements. Hardware requirements will be driven by software performance requirements.

It is anticipated that the system will consist of a network of terminals, a printer, peripherals, software to meet the requirements defined herein, and possibly an external device (i.e. scanner or bar coder) for inspecting fire extinguishers, safety showers, and emergency eyewash stations. In addition, the system will interface with the Bruel and Kjaer 1302 Gas Monitor. This anticipated configuration is depicted in figure 4.1-1.

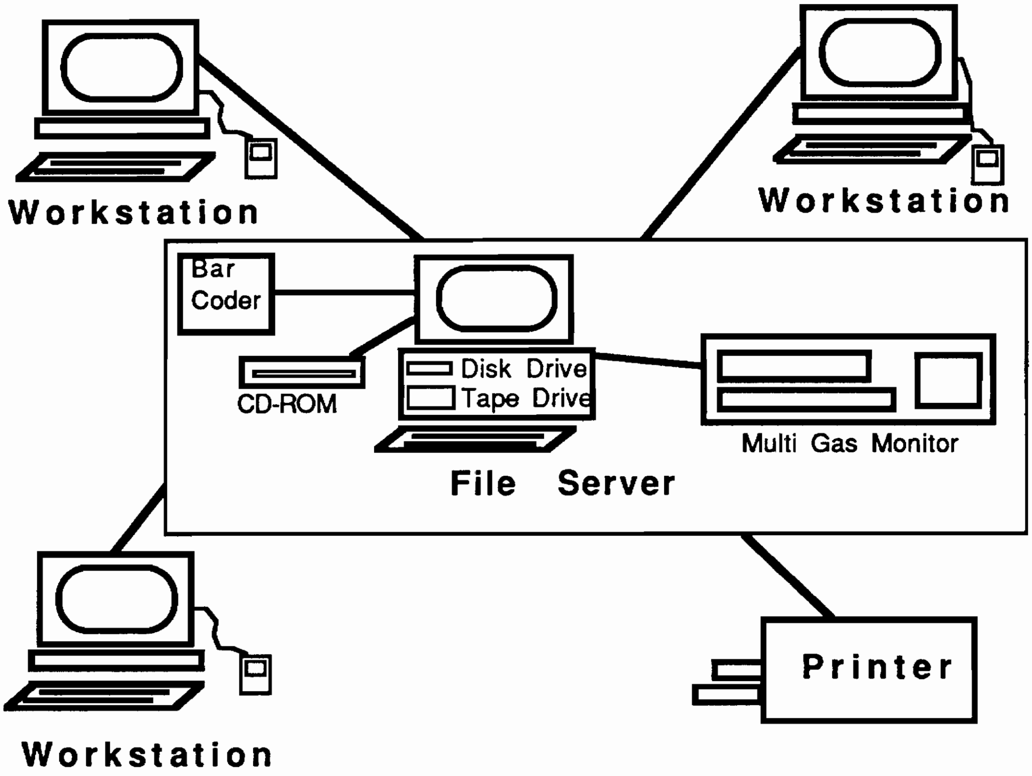


Figure 4.1-1. Anticipated SMITS configuration.

The following sub-sections describe potential usage scenarios.

4.1.1 Scenario One - Chemical Inventory and MSDS

Suppose during a routine material requisition, the forklift carrying the material inadvertently pierces the box containing the material. The forklift operator does not notice the leaking box until he has transported it about 50 meters from the warehouse. He stops immediately and in a panic runs to his supervisor. The supervisor, unsure how to handle the spill, contacts the Safety Office and then runs to cordon off the area.

Simultaneously, the Safety Office accesses the SMITS and searches for the appropriate Material Safety Data Sheet. From the MSDS the Safety Officer determines how to handle the spill and the Safety Officer provides this information to the Spill Response Team who quickly clean up the spill.

4.1.2 Scenario Two - Accident Investigation

An employee, frustrated that the vending machine ate his money, bangs furiously on the machine. Suddenly, his hand is bleeding. He goes to the nurse, and after treating his wound, the nurse sends him by the Safety Office. The Safety Office interviews the man, and as the man answers questions surrounding the incident, the Safety Officer enters the responses into the SMITS. The Safety Officer then generates a report of the incident. No further action is required because the worker's injury resulted from his negligence - there is no corrective action which can be taken to prevent recurrence. However, the SMITS assisted with the investigation and the information is now on the computer to be used for statistics later.

Consider a more serious situation, where an employee jams his finger in a door. An ambulance rushes the employee to the hospital. This situation involves workers compensation. And action is demanded to ensure that this accident does not occur again. The Safety Officer investigates the accident, compiles the information, enters it into the SMITS, and generates the worker's compensation form from the information just entered and a report with recommended corrective action to be distributed and briefed to the parties involved.

Finally, it is now the end of the year and the Safety Office needs to compile statistics. Through the SMITS accident investigation application this is easy. The Safety Officer can access a summary of the number of falls, trips, shocks, burns, etc. numerically and/or pictorially. In addition, the Safety Officer can determine if there were "repeat offenders" - individuals subject to more than one accident or incident.

4.1.3 Scenario Three - Training and EPA Regulations

The Safety Officer turns on his terminal and searches the training database for asbestos training. He examines the dates this group of employees were certified and ascertains that they need to be re-certified with a refresher course within one month or else the certification will expire. He then searches the data base to determine the number of employees still requiring Hazard Communication training, identifies twenty five names and prints the list so that he can notify the individuals and their supervisors and schedule a course.

4.1.4 Scenario Four - The Audit

It is the Monday after the Super Bowl. The workers are a bit sluggish after the late night game but quickly shake off the cobwebs of the night when they notice a man and a woman holding clipboards and wearing wind-breakers emblazoned with "EPA" in big block letters. The two EPA auditors are directed to the Safety Office and demand to see training documentation, chemical inventory, MSDSs, and inspection records. The Safety Officer logs onto SMITS and answers all of the inspectors questions. The inspectors are so impressed with SMITS that the Safety Officer demonstrates the accident investigation capability. The site still gets written up for a minor infraction but the Safety Officer receives a job offer.

4.2 PERFORMANCE AND PHYSICAL PARAMETERS

4.2.1 Efficiency

The SMITS shall respond to the user in a timely manner, displaying a prompt to indicate that it is in the process of doing something within a maximum of 2 seconds so that the user knows that the system is responding and providing the user response within 60 seconds, as time response is critical in emergency situations.

The SMITS shall indicate that the system is processing and provide the capability of actions occurring in the background. For example, while a document or report is printing, the user shall be able to continue to operate the system. The system shall also provide a convenient means of switching between applications and allow more than one document to be opened simultaneously.

4.2.2 Integrity

Government security constraints dictate that the system be safe from non-authorized users gaining access via password protection and physical location. Furthermore, the system shall be designed so that user's can store and access individual data privately, such as a word processing document, which can not be accessed, printed, changed, deleted or viewed by any other user except for the System Administrator. This will allow users to set up private documents and files. Figure 4.2.2-1 illustrates the System Administrator's access to everything, and the users access to common files while maintaining private files as well.

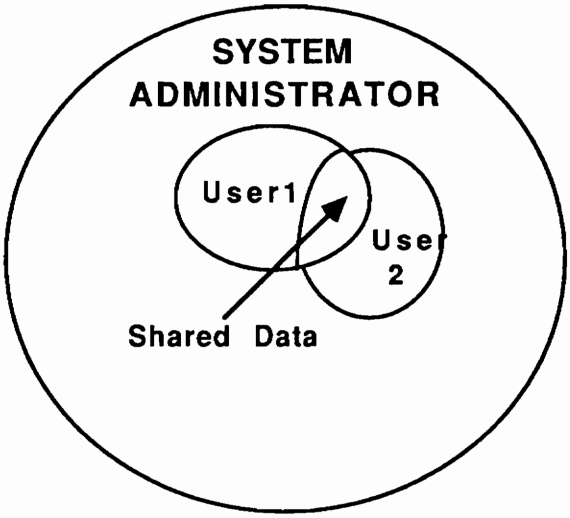


Figure 4.2.2-1. Data access

The system shall be designed so emissions from the hardware (including cabling) remain undetectable at less than 900 feet because of the sensitivity of the data contained on the system.

4.2.3 Reliability

The SMITS shall be a minimum of 85% reliable based on the mission profile of the system operating 11 hours a day for 5 days a week over a five year time frame. Reliability shall be achieved by purchasing high reliability components, uninterruptable power supplies (UPS), redundancy or a combination as determined by the system design. The system shall perform self tests upon start up to verify the system is operating correctly and shall indicate to the user any problems. The problem indications shall be more specific than a go/no go indicator so that the System Administrator can pinpoint the problem. System reliability is important because there will be times when the Safety Office is using the system in an emergency mode.

4.2.4 Survivability

The system shall not lose data in the event of a power failure. Nor shall the system sustain damage or data loss in the event of a power surge or spike.

The system shall provide the capability of instituting regular scheduled back ups.

Any portable SMITS component, such as a hand scanner, shall be capable of withstanding without breakage 1 drop from a 4 foot height on to concrete, operating temperatures ranging from 65 to 120 degrees Fahrenheit and relative humidity typical of the Washington DC area.

4.2.5 Usability

The system shall be more than user friendly - it shall be user harmonious. This shall be accomplished by a combination of menus, graphics, mouse usage, macro keys, readily accessible help, prompts, messages, and easily understandable documentation and training. A non-computer literate individual shall be able to learn how to operate the system within an 8 hour training session. The System Administrator shall be able to intimately learn the system and administrative techniques within a 5 day, 8 hour per day training session.

4.2.6 Maintainability

The Government installation has a cadre of personnel available to support IBM hardware. Government security constraints prevent outside repairs to be conducted. As a result, the system shall be designed so that hard drive and video display unit repairs are obtainable via on-site cleared vendors and replacement parts are available commercially with a lead time no longer than 3 days. The system shall be installed such that items requiring preventive maintenance from site personnel are readily accessible.

4.2.7 Expandability

The SMITS shall have the potential to connect to satellite sites in the Northern Virginia area. The type of system located at the other sites is undefined at this time.

The system shall also be easily capable of supporting and implementing upgrades without more than a half day impact on users.

4.2.8 Flexibility

Each user station shall be able to function as an independent personal computer so that functionality is not lost in the event of a SMITS crash. The system shall be able to accommodate additional user requirements regarding software upgrades and additional packages as well as offering the potential to be integrated with other systems located in Northern Virginia.

4.2.9 Interoperability

The system shall have the capability of interfacing directly with the existing Bruel and Kjaer Model 1302 Multi-Gas Monitor and supporting the BK Link Software. The 1302 has both an IEEE-488 parallel and an RS-232-C serial interface. The IEEE-488 interface is designed in accordance with the recommendations of IEEE Std 728-1982, "IEEE Recommended Practice for Code and Format Conventions". The RS-232-C interface connector is a 25-pin D-range male connector, and has potential baud rates or speed of transmission of: 300, 600, 1200, 2400, 4800 and 9600 bits/second. The 1302 can convert data received on the serial interface into data which can be sent out on the IEEE 488 parallel interface. The BK Link Software is designed to operate on an IBM PC or compatible. Because the software is available only for IBM PC the design of the system shall ensure that the software is usable, either through hardware selection or modification of the existing software.

4.2.10 Portability

If bar coding is selected as a means of meeting user requirements, the bar coding component shall be portable. No other system components need to be portable, however, they do need to be moveable in the event of office relocation.

4.2.11 Size

The system size shall be such that portable components are not cumbersome. Additionally, workstation components shall conform to typical PC sizes and Video Display Units shall be a minimum of 14 inches to facilitate the user interface.

4.2.12 Weight

Portable components of the system shall weigh no more than 1 pound. If portable components interact, the combined weight for these components shall be no more than 5 pounds so that individuals do not suffer from fatigue.[1]

4.2.13 Speed

The system shall react to user input within 60 seconds. The system shall display a prompt to indicate that it is in the process of responding to the user within 2 seconds. Database queries shall require no more than 3 seconds. The printer shall be capable of printing a minimum of 4 pages per minute.

---

[1] Suzanne H. Rodgeers, *Ergonomic Design for People at Work* (New York: Van Nostrand Reinhold, 1983), p. 152.

4.2.14 Accuracy

Data accuracy is critical to the safety programs functions. Inaccurate data could result in spreading a disaster rather than eliminating it. However, the accuracy of data is highly dependent upon the operator(s). As a result, the system shall be designed to allow the operator to verify and change data to ensure accuracy of input and output.

4.2.15 Capacity

The system shall be able to accommodate at a minimum 2 times the amount of memory dictated by commercial software, word processing, spreadsheets and database requirements to provide for future growth[1].

4.3 USE REQUIREMENTS

Figure 4.3-1 depicts anticipated use of the SMITS.

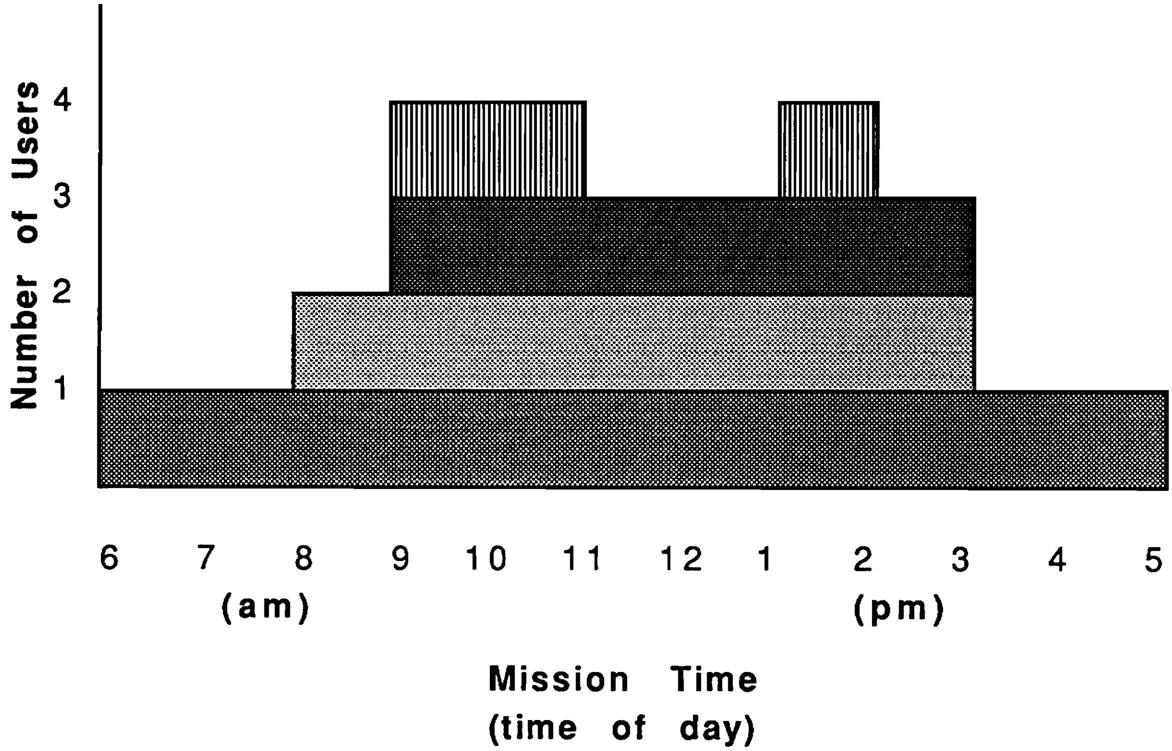


Figure 4.3-1. SMITS Mission Profile.

---

[1] Braunstein.

The system will be accessed continually throughout each working by at least two users and a maximum of four users. Daily operational time will be approximately 11 hours, five days a week (Monday through Friday). The system will not be used on the weekends, unless there is an emergency. An emergency requiring the attention of the Safety Office outside of normal working hours occurs an average of 5 times per year.[1]

4.4 OPERATIONAL DEPLOYMENT

The SMITS shall be capable of supporting simultaneously, 4 Safety Officers at a Government site in the Northern Virginia area. The system, once installed will be stationary unless offices are re-configured, in which case the system will be moved to a new office on the same Government site. All users will be located in the same 5,399.56 square foot area;..

If the design concept analysis yields a method such as scanning or bar coding for inspecting extinguishers, eyewashes and safety showers this interface shall be portable.

Four people shall have access to the system - including the hardware, software and peripheral interfaces. The system shall be fully operational no later than 31 December 1993.

It is desirable that the system have the potential to interface with other classified Government systems in the Virginia area. These systems do not exist at this time; however, the SMITS should be built with future connectivity considered.

4.5 OPERATIONAL LIFE CYCLE

The SMITS shall be operational until 31 December 1998, at a minimum. A five year life cycle is used in anticipation of significant technological advancements, such as secure means of wireless LANs, that will be desirable to incorporate into the safety system. The SMITS will be used by Safety Office personnel and shall be capable of supporting 4 users simultaneously. Throughout the system life cycle the

---

[1] David Nay, interview, Springfield, Virginia, 25 February 1993.

system shall be operated in accordance with the use requirements defined in Section 4.3. The system shall be designed so that it can support one intermediate software up-grade to accommodate major changes in the software. Although updated software may be released sooner, it is not cost effective to be continually upgrading software.

It is not anticipated that the requirement for the system will become obsolete at the end of the operational life cycle; rather, it is anticipated that hardware and software technology will have advanced. In addition, it is highly probable that additional requirements will be developed during the operational life cycle. As a result, it is anticipated that towards the end of the operational life cycle a follow-on or SMITS upgrade will occur.

4.6 EFFECTIVENESS FACTORS

Reliability, like maintainability is a function of the system's design. Reliability is defined as the "probability that a system or product will perform in a satisfactory manner for a given period of time when used under specified operating conditions."[1] In the case of a computer based information system, the reliability of both hardware and software must be considered.

Table 4.6-1 contains the required reliability and maintainability requirements derived from the requirement of overall SMITS reliability of 85%.

Table 4.6-1. Effectiveness factors.

RELIABILITY FACTORS	REQUIREMENTS
Mean Time Between Failure	87,990 hours
Mean Time Between Maintenance	54.9 hours
Operational Availability .	.9565
MAINTAINABILITY FACTORS	**REQUIREMENTS**
Mean Preventive Maintenance Time	19 minutes
Maintenance Down Time	2.5 hours

---

[1] Blanchard, p. 347.

Since the reliability, R, is required to be .85, the Mean Time Between Failure (MTBF) is derived, using the relation:

$$R = e^{-\text{MTBF}/t} \qquad [1]$$

where t, the operational life time is 5 years for 11 hours a day, 5 days a week or 14,300 hours. The Mean Time Between Maintenance (MTBM) is found from the relation:

$$\text{MTBM} = 1/\left(1/\text{MTBF} + 1/\text{MTBSM}\right) \qquad [2]$$

where the MTBSM or Mean Time Between Scheduled Maintenance is specified as 55 hours (see Maintenance Concept).

The operational availability (A_o) is the "probability that a system or equipment when used under stated conditions in an *actual* operational environment will operate satisfactorily when called upon"[1] is determined from the relation:

$$A_o = \text{MTBM} / (\text{MTBM} + \text{MDT}) \qquad [3]$$

where:

MTBM = Mean Time Between Maintenance and

MDT = Maintenance Down Time

Using the worst case scenario for specified MTBM and MDT, the minimal operational availability the system must meet is calculated to be 95% using equation 3.

The Mean Preventive Maintenance Down Time (MPMT) is "the elapsed time to perform preventive or scheduled maintenance"[2] is calculated to be 19 minutes (when neglecting the one time occurrence of an 8 hour system upgrade and the infrequent log-on requests) using the relation:

$$\text{MPMT} = \text{sum}(\text{Mpt}) / (\text{Np}) \qquad [4]$$

where:

Mpt = active maintenance down time per preventative maintenance task

Np = number of maintenance actions

---

[1] Blanchard, p. 359.

[2] Blanchard, p. 401.

Note that this is the mean time per preventive maintenance actions calculated using the maintenance actions specified in the maintenance concept (section 7.4.1).

4.7 ENVIRONMENT

The system shall operate in a normal office environment, with temperatures ranging from 70-74 degrees Fahrenheit. If there is an automated, transportable method for inspecting fire extinguishers, safety showers and emergency eyewashes the temperature range for this system interface shall extend from 65-120 degrees Fahrenheit and the relative humidity range the equipment is exposed will vary from 0 to 70 %.

4.8 HUMAN FACTORS

The system shall be designed to optimize the man-machine interface. Because static work postures cause fatigue, workstations shall be configured so that they are adjustable to accommodate the user's size. Similarly, because repetitive motion can lead to nerve damage, keyboards and mice shall be selected to minimize the risk of injury. Screen glare causes headaches, blurred vision and eyestrain;[1] consequently, the system shall be designed to minimize glare. Concerns over electromagnetic radiation emanating from terminals shall be mitigated by maintaining a minimum distance of 2 feet between the user and the video display terminal.

---

[1] Laurel Touby, "Is your office a health hazard," *SELF,* (September 1992), p. 105-108.

5.0 FUNCTIONAL ANALYSIS

5.1 OVERVIEW

The operational requirements (such as 4 users having access to the same information simultaneously, and system response time of 60 seconds) dictate that the safety management information and tracking system be an integrated entity consisting of hardware and software. The system is divided into three subsystems:

1. the workstations, file server and peripherals;
2. the application and operating software; and
3. hardware interfaces, including the Multi Gas Monitor.

Each of these subsystems must perform critical functions in conjunction with the other subsystems for the proposed design to achieve success in its mission.

The functional analysis "constitutes the process of translating operational and support requirements into specific qualitative and quantitative design requirements."[1] The objective of the functional analysis and subsequent generation of functional flow diagrams is to ensure the design, development, and system definition proceed logically. Blanchard recommends that "not one piece of equipment be defined or acquired without first justifying its need through the functional requirements definition process."[2] For SMITS, the functional analysis must address the actions of each subsystem with regard to operations and maintenance as they work synergistically to meet the Safety Program goals.

5.2 ABBREVIATED FUNCTIONAL ANALYSIS

The objective of the functional analysis is to aid in the identification of " the method for accomplishing the various functions- manually, automatically, or a combination thereof, and to identify the resources required to accomplish the function...functional flow diagrams indicate

---

[1] Blanchard, p. 57.
[2] Blanchard, p. 57.

basic system organization and ...identify functional interfaces."[1] Normally, functions are broken down to the level which establishes the needs of the system; however, for the SMITS preliminary analysis, only operations and maintenance functional flows are employed. Figure 5.2-1 depicts the SMITS top level function series.

Each of the functions in figure 5.2-1 can be broken down to another level. Consider, for example, the operational function. This occurs after the SMITS is installed and users are implementing the system. Figure 5.2-2 illustrates the functions at level 2 and level 3.

The maintenance function, from figure 5.2-1 can also be broken down into levels. Figure 5.2-3 depicts the maintenance functions at the first level.

Prior to system detailed design, this iterative process will continue for each function until the needs of the SMITS are established and the system can be designed from the functional analysis.

---

[1] Blanchard, p. 57.

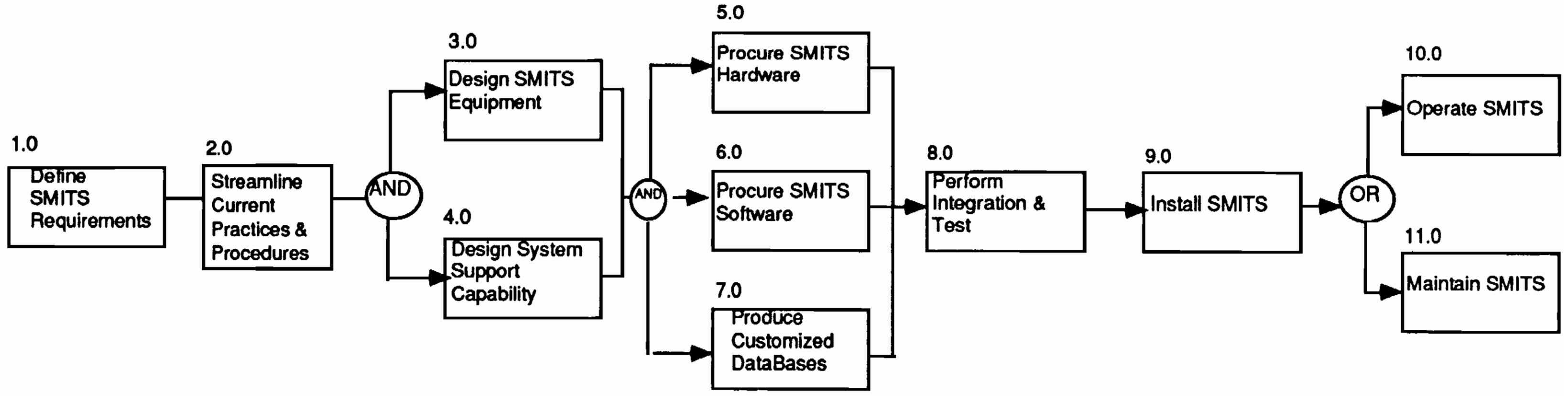


Figure 5.2-1. SMITS top level functional analysis.

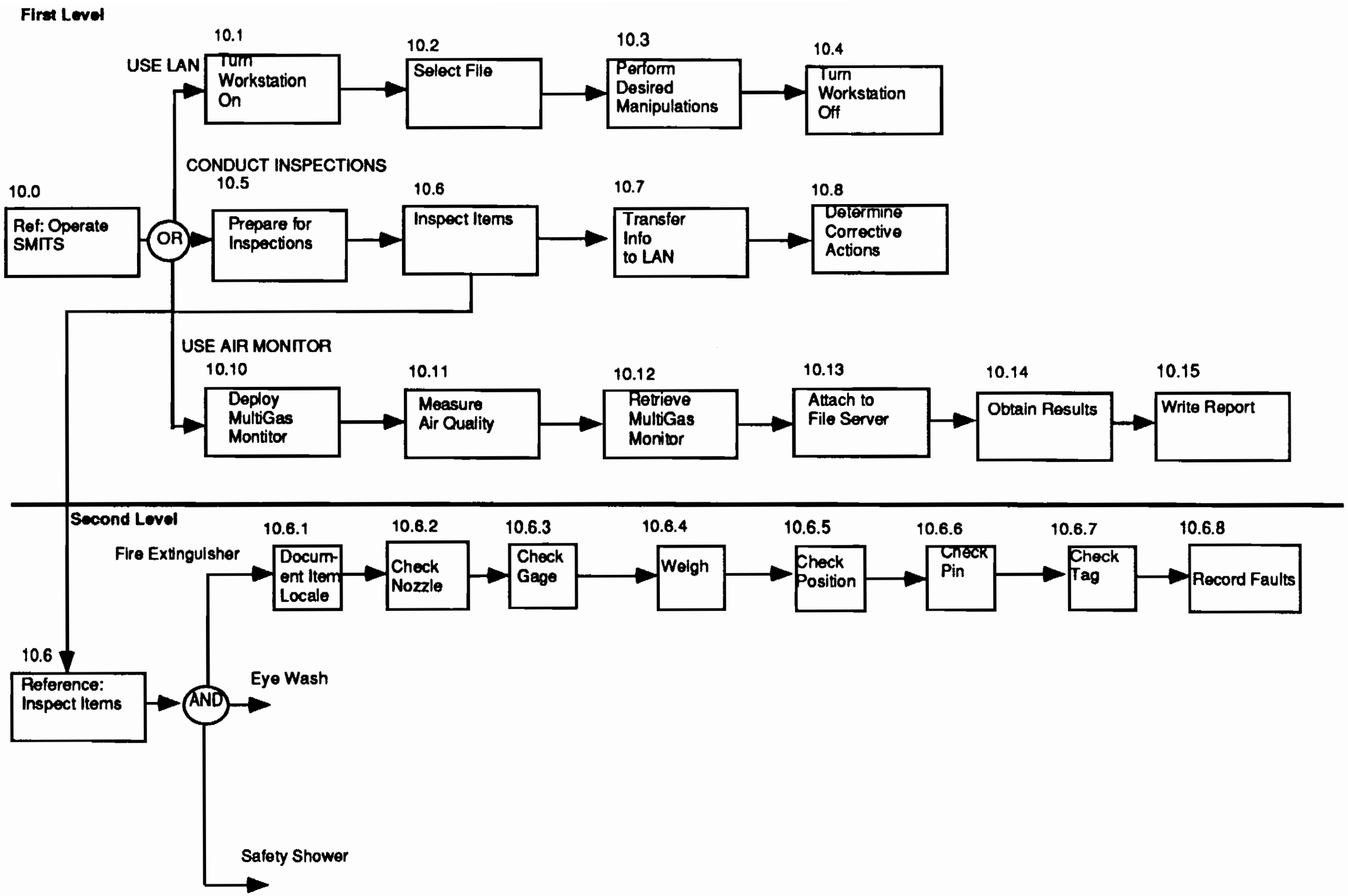


Figure 5.2-2. First and second level abbreviated operations functional analysis.

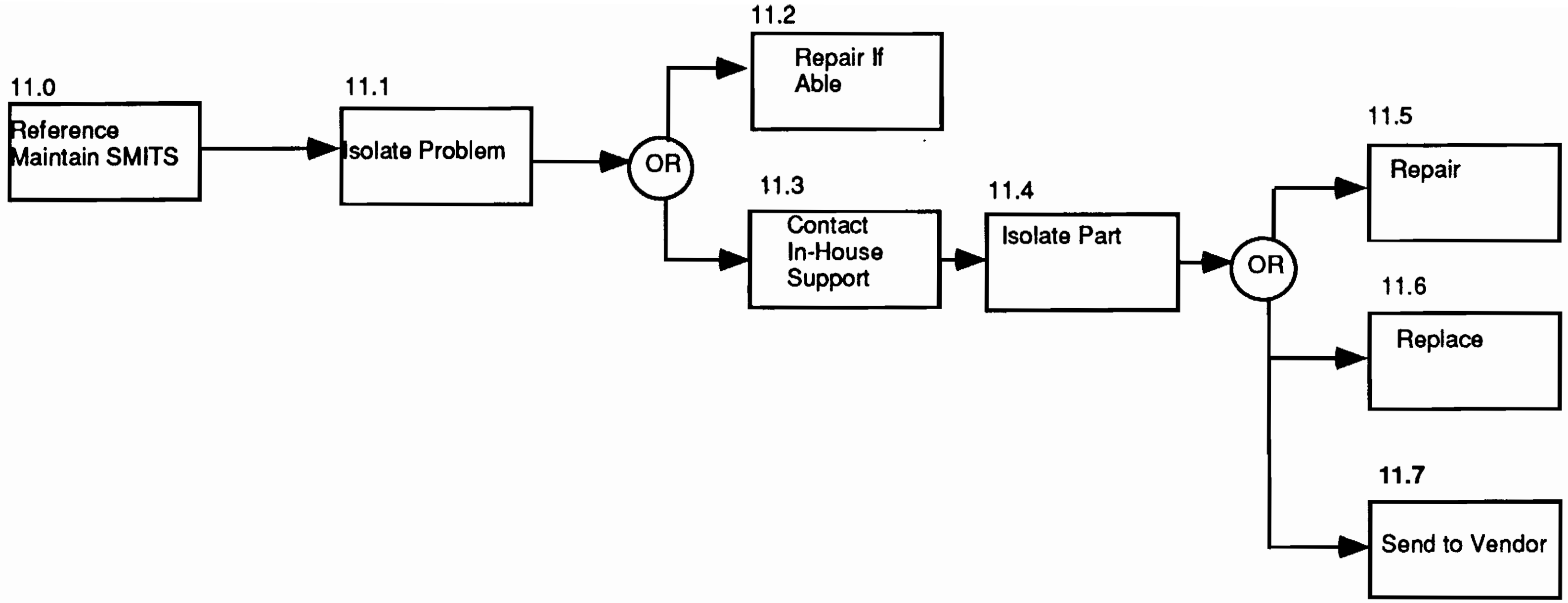


Figure 5.2-3. Maintenance concept functional analysis.

6.0 CONCEPT DEFINITION

6.1 INTRODUCTION

The feasibility analysis identified several potential solutions to solving the current deficiencies of the Safety Program. The functional analysis translated the user operational and maintenance requirements into a logical function flow. In order to develop a preliminary design concept for the SMITS, trade-offs are addressed along with applicability to user requirements. Work simplification, computer platforms, peer-to-peer networks, automation and bar coding are examined and a recommended design concept developed.

In order to design the SMITS, the limitations as well as the nature of the Safety Management Information and Tracking System, as depicted pictorially in figure 6.1-1, must be understood.

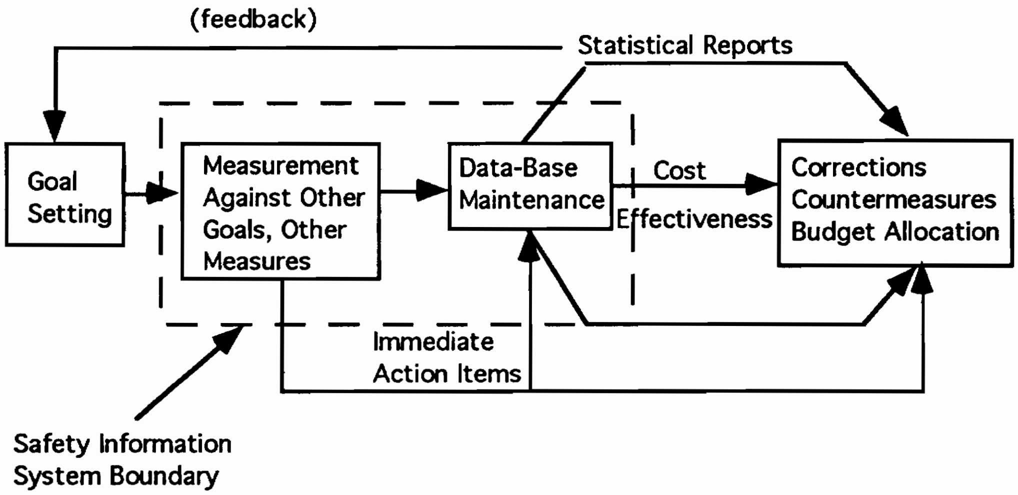


Figure 6.1-1. SMITS boundaries.[1]

The measurement and evaluation functions are performed directly by the safety system, while the goal setting and correction functions are influenced by SMITS. SMITS is "a means to an end and not an end in

---

[1] David Brown, *Systems Analysis and Design for Safety* (Englewood Cliffs: Prentice-Hall, Inc., 1976), p. 248.

itself".[1] By not losing sight of this, the implemented SMITS will avoid the pitfall of so many other information systems: failure to provide useful information for control.

6.2 WORK SIMPLIFICATION

Work simplification provides an easy, inexpensive means to improve the processes of the Safety Program. Prior to automating the existing Safety Program, the procedures and processes should be challenged to determine if there is a better way of achieving the same, or improved, results. It does not make sense to spend thousands of dollars automating a process which is inefficient. Furthermore, application of work simplification techniques may reveal that the improved process does not necessitate automation. Work simplification techniques can be applied to both paper work and non-paper processes

Consider, for example, the Safety Program accident/incident investigation and reporting process. The existing process is defined in figure 2.2-1. Applying paper work simplification techniques yields the process pictorially represented in the information process chart contained in figure 6.2-1. After analyzing the process and applying the work simplification questions and challenge, one wonders why it is necessary to fill out three forms - especially considering the duplication of information. Figure 6.2-2 depicts a streamlined paper flow, eliminating the Site Accident Form by modifying the Nurse Accident Form (NAF) so that Safety adds additional information to the NAF rather than creating an entirely separate form. This process still requires automation in order to meet operational requirements, such as statistical generation. Furthermore, since there is duplicate information across the workers compensation form as well (see section 2.2 for sample original forms) automation will allow the information to be entered once and then generate various forms.

---

[1] Brown, p. 248.

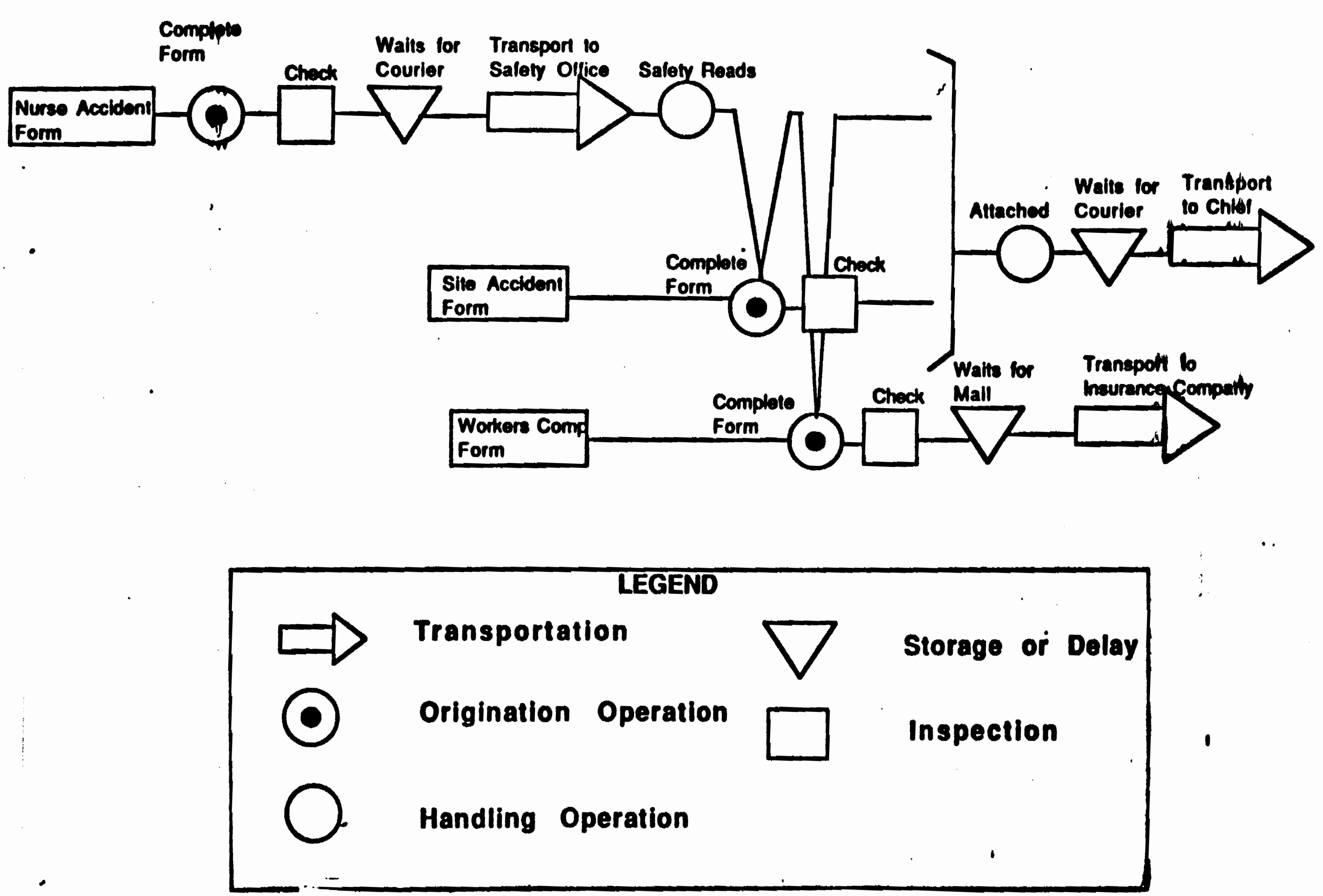


Figure 6.2-1. Accident investigation paper work.

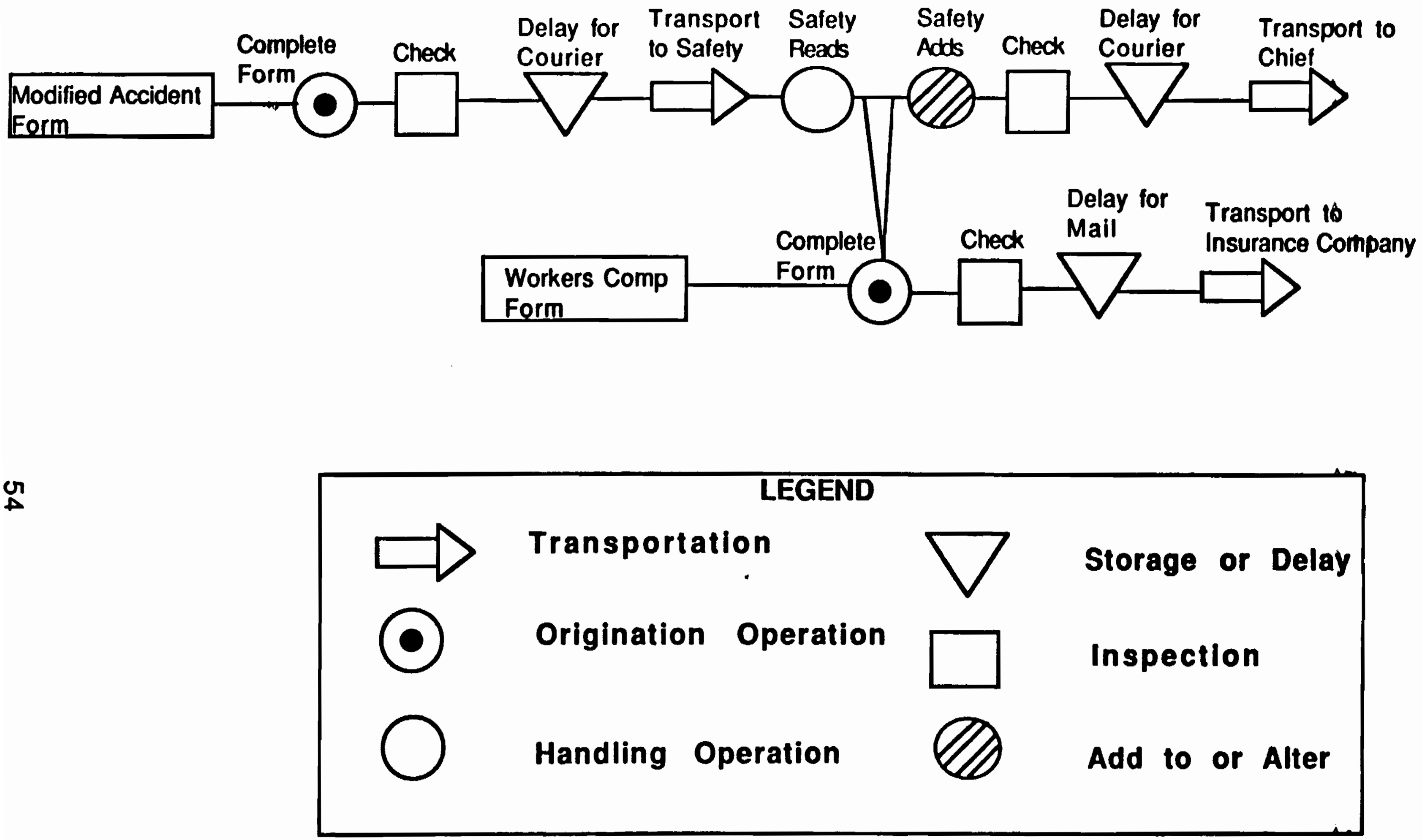


Figure 6.2-2. Streamlined accident investigation paper work.

Prior to automation, **all safety processes should be subjected to the work simplification technique** to ensure that each process being automated makes sense. Ben S. Graham, Sr. said, in 1957, "In preparing for paperwork automation we must first get the water out of our systems, eliminate the waste, and in doing it make savings equal to, or even in excess of, our annual profits. The next step is to determine our need for equipment." Furthermore, the "water" must remain out of the system - to help ensure that the SMITS stays effective, workers will continually use the work simplification techniques to constructively challenge processes, providing feedback needed to measure and monitor the performance of the safety system itself.

6.3 EXISTING SYSTEMS

A preliminary survey of the market did not reveal the existence of a comprehensive safety information system available for purchase. Many companies, as addressed in Section 3, have developed their own, unique safety system, either automated or not, which satisfies *their* requirements. However, as discussed in Section 3, these systems have limitations or other constraints which prevent adaptation to the Government Safety Program. Additionally, there are several software packages available on the market to assist with federal compliance, but no package satisfying the Safety Program demands was identified.

Using the lessons learned from other safety systems, such as using broad categories to categorize accidents, users will help to avoid the same mistakes in SMITS design.

6.4 AUTOMATION

Automation will facilitate the Safety Program tasks and functions. However, there are several factors to consider regarding automation, such as computer platforms, peer to peer networks, Local Area Network topology and media access control and custom and commercial software. These are addressed in the ensuing sections.

6.4.1 Computer Platform

Operational interface requirements dictate the computer platform be either IBM or compatible (section 4.2.9 specifies external interface requirements for connection to the Bruel and Kjaer Multi Gas Monitor and operating the BK Link Software). Using an IBM or compatible facilitates maintenance as well since the Government employs IBM technical support on-site.

Consequently, **the system will be based on IBM or compatible hardware.**

6.4.2 Computer Connection - Peer-to-Peer versus File Server

Operational requirements indicate that the users are going to be accessing the same database files and OSHA and EPA regulations. Since each user is sharing more than the printer, peer-to-peer resource sharing is not a viable solution. Therefore, **SMITS will use a file server.**

6.4.3 LAN Standards and Media Access

The protocol standard drives Media Access Control and physical and logical topologies. There are two IEEE standards: 802.5, addressing Token-Ring architecture and 802.3 using carrier sense multiple access medium access control (MAC) scheme. 802.3 is derived from the earlier Ethernet system and while Ethernet is a subset of 802.3 the two terms are often used synonymously. The LAN adapter or network interface card (NIC) conforms to one of these standards, and influences many other network decisions.

Each computer which is on a network needs a *LAN adapter* or printed circuit board which goes into an expansion slot in the computer to provide the mechanical and electrical connections between the computer and the network. The LAN adapter card actually translates the low-powered electrical signals which are moving in parallel inside the computer into serial data to flow through the LAN cable, and visa versa. The LAN adapter dictates the type of wire or *media* needed for the network and the method of *media access* which is the way the nodes or clients access the media.

Token-Ring installations tend to be more costly than Ethernet and Ethernet offers efficient ways to connect to various computer systems.[1] Since flexibility to connect to other systems in the future is a requirement, **Ethernet adapter card is the best alternative for SMITS.**

Medium Access Control (MAC) defines the method for determining which terminal has access to the transmission media at any time. Two MAC techniques are:

- Carrier Sense Multiple Access with Collision Detection (CSMA/CD);
- Token

CSMA/CD operates in a listen prior to transmission mode. Prior to sending data, the network adapter checks to determine if any other node or terminal is trying to transmit. The network adapter accepts the broadcast message only when the cable is quiet. If two or more terminals simultaneously transmit, resulting in a collision, the network adapter is able to detect the collision due to the resulting high electrical-signal level and the network adapter cards send jam signals to ensure that the conflicting nodes are aware of the collision. The adapter card at each node terminates transmission and randomly selects a re-transmission time to ensure the nodes don't continue to transmit colliding signals every time the cable is free.

Token MAC is divided into token bus and token ring. Although similar, the processes differ because of the different topology. With the token bus, the nodes form a logical ring. A token circulates through the ring and nodes receiving the token can transmit and then must pass the token around. Similarly, in the token ring technique a token circulates through the ring and stations transmit by capturing the ring, inserting a packet onto the ring and then passing the token on.

As a result of selecting 802.3 as the driving standard, **CSMA/CD is the MAC scheme** for SMITS.

---

[1] Derfler, p. 123.

6.4.4 Topology

LAN *topology* is the structure that provides the communications interconnection among the terminals or nodes on the network, defined by the physical layout of switches and cables. The most common topologies are the *star*, *bus* and *ring*, as depicted in figure 6.4.4-1.

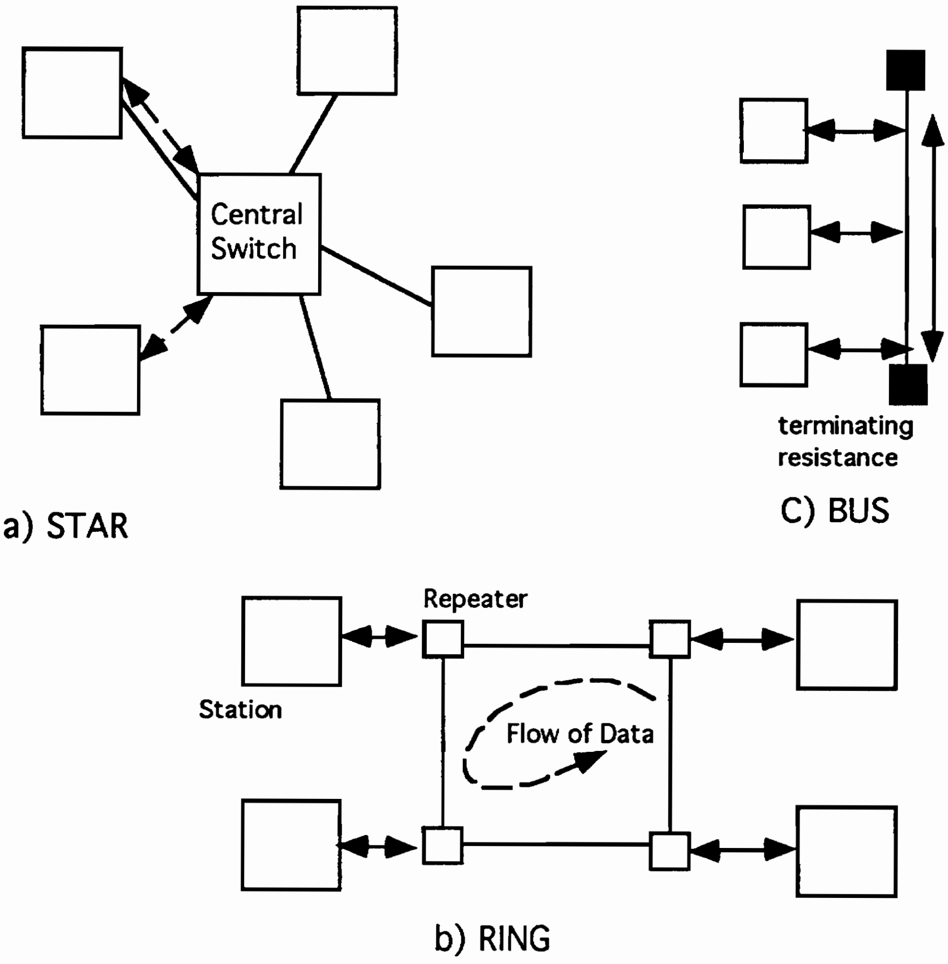


Figure 6.4.4-1. LAN Topologies. [1]

In the star topology communications are centralized as nodes connected to a central switch; transmission occurs by asking permission from the central switch which then establishes the circuit. The bus

---

[1] William Stallings, *Local Networks*, p. 65.

topology relies on the communications network to function as the transmission medium. All nodes are attached directly to a linear transmission medium known as the bus. Transmissions are divided into packets and only one node can transmit at a time. The ring topology consists of repeaters joined by point-to-point links which circulate in only one direction. Transmission data is broken into packets containing the destination address and passed from point-to-point until it reaches the destination; the destination recognizes it's address and copies the packet.

The star topology offers the advantage of survivability and reliability; the network wires run between the network nodes and a central wiring hub which isolates wiring. Even if a wire between a workstation and the hub breaks, the rest of the network remains operational. Furthermore, the overall installation is usually neater and easier because fewer wires run into each node than other configurations such as the bus.[1]

The common physical topology associated with Ethernet is either the daisy chain (bus) or the star. Although the star requires more cabling than the bus, the cost of the additional cable is minimal when weighted against the importance of survivability. Consequently, for SMITS, the **star topology** is recommended.

6.4.5 Media

Each workstation is connected to the file server via media. There are currently four types of connection:

- twisted pair, which is phone wire - two insulated copper or copper coated steel wires in a spiral pattern, twisted to minimize electromagnetic interference between the pairs;
- coaxial cable, which consists of a hollow outer conductor that is solid or braided wrapped around a single inner wire conductor that is either solid or stranded - coaxial cable operates over a wider frequency range than twisted pair;

---

[1] Derfler, p. 115.

- fiber-optic strands, which are made of glass fibers surrounded by strengthening materials and offer the advantages of eliminating electrical interferences, carrying vast quantities of data over long distances at high speeds and a small diameter; and
- wireless connections, which rely on radio frequency transmissions and application to computer systems is fairly new and relies on high frequency transmission which has security impacts (i.e. signals can be intercepted) and as a result will not be considered as an option for SMITS.

Table 6.4.5-1 compares the cable types for the SMITS application.

Table 6.4.5-1 Media comparison.

MEDIA	ADVANTAGE
Twisted Pair	None. Although cheap, installation costs dwarf material costs. Existing telephone wiring at Government site not usable.
Coaxial Cable	Medium cost, more immune to noise than twisted pair, thin coax is flexible
Fiber Optic	High cost, immune to noise, good for long distances

Analysis of table 6.4.5-1 leads to the selection of **coaxial cable** for SMITS since long distance is not required and noise impacts are minimal.

6.4.6 Summary of Recommended Hardware Design

Figure 6.4.6-1 depicts the recommended SMITS hardware.

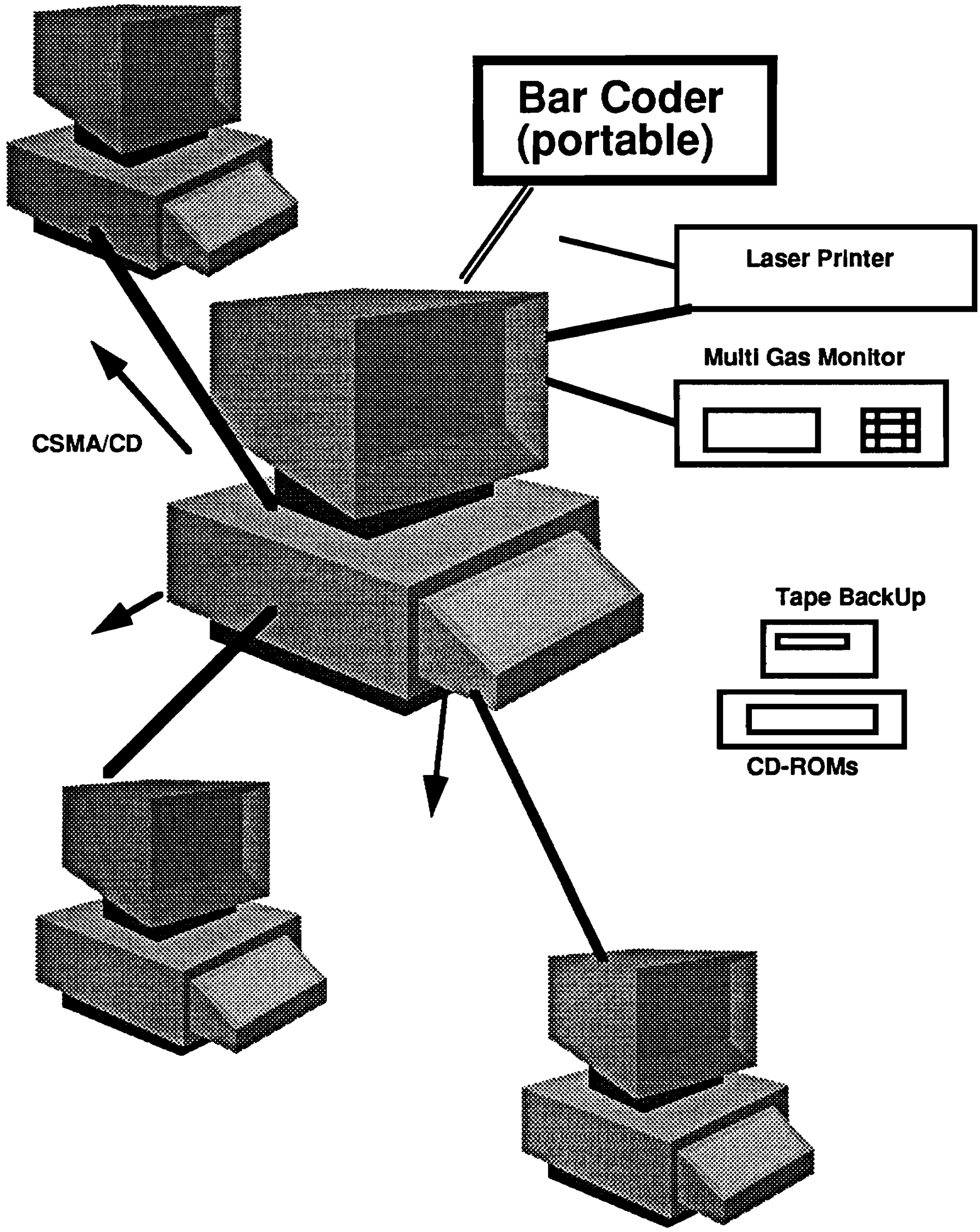


Figure 6.4.6-1. SMITS hardware configuration.

Three IBM PC or compatible workstations and one file server will be configured in a star topology using Ethernet adapter cards, CSMA for access control and coaxial cable for connection. The file server will also act as a workstation. Using the flow chart in figure 6.4.6-2 as a sanity check leads to the same results regarding adapter cards.

6.4.7 Software

Operational requirements dictate the need for many software packages: electronic mail, word processing, security (i.e. password protection), and data base capabilities. First of all, the network needs an operating system. Users and computer experts all agreed Novell 3.11[1] is the best package for SMITS requirements and it has inherent security and electronic mail capabilities. There are other packages, such as Banyan Vines, but they do not receive the same high ratings as Novell 3.11.

For application software, prices are inexpensive and technical support is available via toll free numbers; the best thing to do is use commercially available packages, such as Microsoft (MS) Windows for user interface requirements, MS Word for word processing and MS Excel for spreadsheets.

Tracking training requirements, accident investigation and reporting, and survey tracking each require a database package to be customized for application. There are commercially available packages for accident investigation and reporting through the National Safety Council such as Accuse 2.1, however, this package costs $1,295. For $99 MS Access or Borderland Paradox for Windows can be purchased. Then, required databases for SMITS could be developed using the database package. It is estimated that the database development and testing would require the attention of a junior computer engineer for 2 weeks, at a cost of $1200. The total cost for the three databases would then be $1299. Figure 6.4.7-1 shows a comprehensive input prototype (note that this report can be modified to improve appearances and facilitate question flow) and figure 6.4.7-2 sample report generated using a commercially available database package.

---

[1] Joe Lyczak, FDA telecommunications specialist, telephone interview, 2 March 1993.

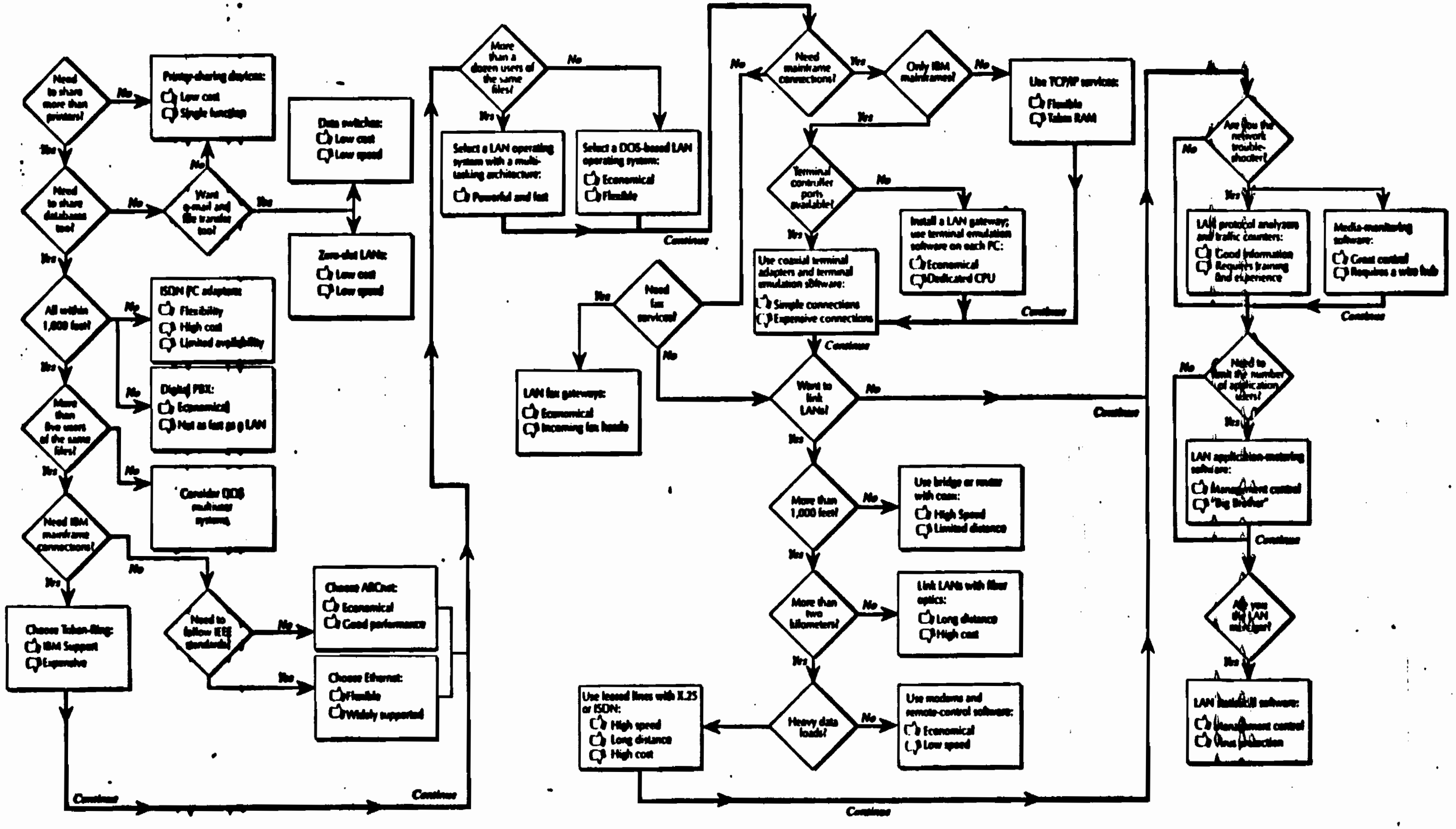


Figure 6.4.6-2. Connectivity decision tree.

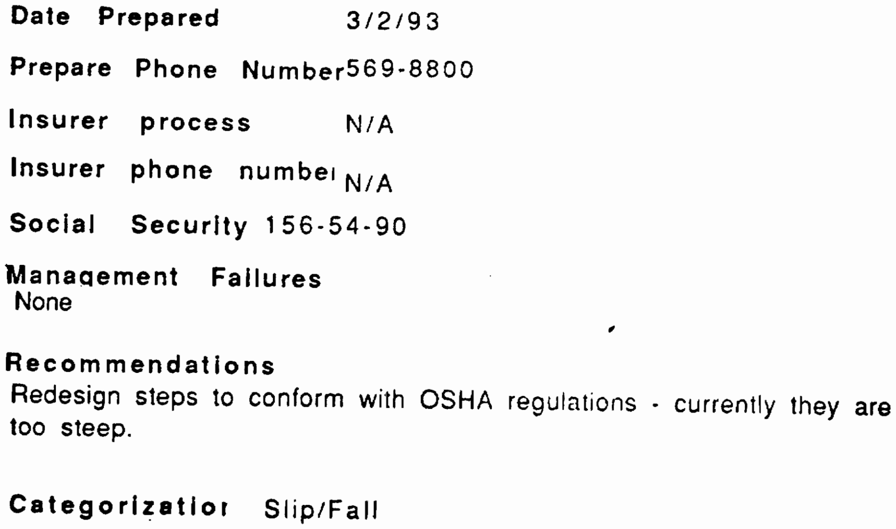
Comprehensive Accident Investigation Data

Employer	General Electric
Federal Tax Id	9270Qj
Employers case #	N/A
Employer Street Addres:	8080 Grainger Court
Employer City	Springfield
Employer State	Va
Employer Zip	22153
Location of Accident	UTB Steps
Parent Company	N/A
Nature of Busines	Aerospace
Insurer	Electric Mutual
Policy Number	N/A
Effective Date	N/A
County Accident Occure	Fairfax
On employer premises	YES
On state property	NO
Accident Date	2/26/93
Accident Time	1600
Date of Incapacit	2/26/93
Hour of Incapacit	1600
Employee paid in full?	Yes
Employee paid for incapacity?	Salary
Date injury reported	2/26/93
Person to whom reporte	David Nay
Name of witness	N/A
Death date	00/00/00
Employee Last Name	Jones
Employee First	Steve
Employee Middle	A
Phone number	569-8800
Sex	Male
Employee Street	3000 S. Randolph Street #121
Employee City	Arlington
Employee State	Va
Employee Zip	22206
Employee Birthdat	11/22/68

Figure 6.4.7-1. Sample comprehensive input for accident database.

Marital Status	Single
Occupation at time of injury	Systems Engineer
Department	SMP
Number of dependent	0
No of years in current positic	3
No of years with current	5
Pay method	Salary
No hours worked/day	8
No of days work/week	5
Value of: Food	N/A
lodging	N/A
tips	N/A
other	N/A
Machine or Tool Type	N/A
Specify part of machir	N/A
Safeguards provided?	N/A
Safeguards Used?	N/A
Description of Accider	Tripped on stairs
Nature of Injury	Sprained Ankle
Physician Last Name	Foot
Physician First	James
Physician Street	1600 N. Oak Street Suite 4
Physician City	Arlington
Physician State	Va
Physician Zip	22294
Hospital Name	Jefferson
Hospital Street	
Hospital City	
Hospital City	
Hospital Zip	
Probable length	6-8 weeks
Emp returned to	Yes
At what wage	same
On what date	3/2/93
Prepared by Last Name	Nay
Prepared by First Name	David
Preparer Title	Senior Safety Engineer

Figure 6.4.7-1. Sample comprehensive input for accident database.



Date Prepared 3/2/93

Prepare Phone Number569-8800

Insurer process N/A

Insurer phone numbe N/A

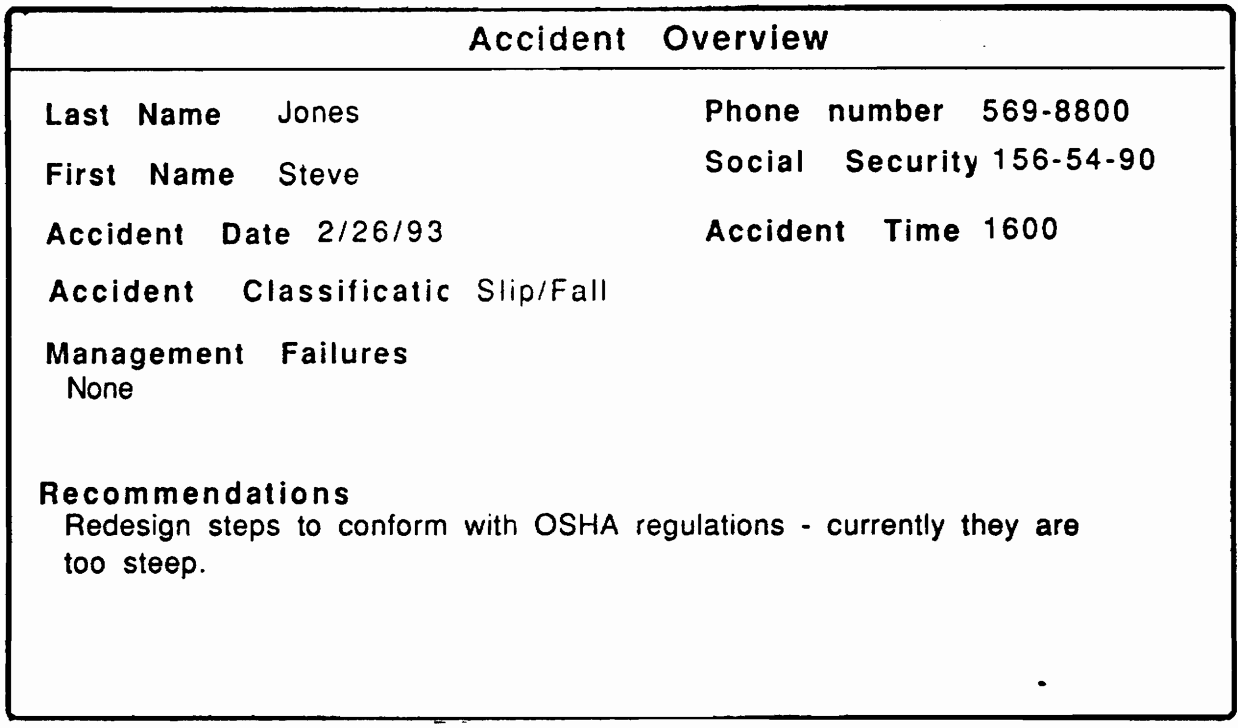
Social Security 156-54-90

Management Failures
None

Recommendations
Redesign steps to conform with OSHA regulations - currently they are too steep.

Categorizatio Slip/Fall

Figure 6.4.7-1. Sample comprehensive input for accident database.



Accident Overview

Last Name Jones

First Name Steve

Accident Date 2/26/93

Accident Classificatic Slip/Fall

Phone number 569-8800

Social Security 156-54-90

Accident Time 1600

Management Failures
None

Recommendations
Redesign steps to conform with OSHA regulations - currently they are too steep.

Figure 6.4.7-2. Sample output for Government report.

OSHA and EPA regulations are available on CD-ROM disks. Subscribing to a service for a year is $5,695 using IHS Regulatory Products. This includes monthly updates, weekly newsletter, on-site training and toll free support. However, regulations are not often changed significantly; because this and the high cost, this service will only be ordered twice during the SMITS lifetime. Similarly, MSDSs are available on CD-ROM through NCTAMS LANT for $76 per year; which includes updates quarterly updates. Both of these products function as databases so SMITS users can search through the data on key words.

6.4.8 Bar Coding

One means of facilitating inspection of fire extinguishers, safety showers and emergency eye-washes is bar coding, as addressed in the feasibility study. Prior to implementing a bar code system, **work simplification should be applied to develop the optimum process for inspections**, as no process exists. It is estimated that using a bar coder will reduce the work load by 50% through decreased inspection and repair time.

Each item at the Government facility would receive a unique number or code identifying it. These codes could be serial or even randomly generated. This code is similar to a social security number. Just like your social security number follows you everywhere, and everyone has a unique number, this unique code, which is adhered to the item, would follow the item everywhere. A database would be established and the code and location linked. The database would then track the location, the status (i.e. discharged, missing pin, improperly mounted, missing component, okay), the date and the inspector's initials. An inspector would scan the code on the item using the hand-held scanner and then scan the menu for the appropriate status of the item. After completing inspections, the information is downloaded to a PC workstation and the database is maintained on the LAN.

There are various types of bar coders available. For SMITS purposes, a non-contact scanner is best because there will be times when the bar code label is difficult to access. Bar code systems can be purchased as independent components, such as scanner, software, label generator software, and labels, or they can be purchased as a comprehensive system. This is similar to buying all of the components to a computer and building it yourself or purchasing a pre-fabricated system.

"Turn key" bar coding systems are available which are tailored specifically to fire and life safety and require very little training. Because the SMITS users are not technically oriented, **a "turn key" system, such as the one sold by Facility Management Systems, is the best bet**. Although turn key systems are more costly, they include support, training, labels and consulting. The Safety Program users will be able to implement this system quicker and more efficiently with this type of service.

6.5 Memory Requirements

Once all of the system specifications are defined and database fields identified, the amount of memory needed for the LAN should be determined. There are two types of computer memory: Random Access Memory (RAM) and Read Only Memory (ROM). RAM is used to execute application programs, such as the word processing package, MS Word. It is used to store programs and data being used by the CPU to run the different programs as requested. ROM is memory containing pre-loaded programs that cannot be rewritten or altered by the central processing unit - such as the routines which get the computer up and running after power up.

Commercial packages specify the amount of RAM and ROM required to run the application. The amount of ROM required for custom developed databases is estimated using the rule of thumb that each character stored in the database requires one byte. Using this rule, database memory requirements are estimated, using the form in figure 6.4.7-1. Table 6.5-1 contains memory requirements for the software required for SMITS.

Table 6.5-1. SMITS memory requirements.

APPLICATION	RAM(MB)	ROM(MB)
Operating System (i.e. Novell 3.11)	8	10
Windows (i.e. MS Windows)	4-8	15
Word Processing (i.e. MS Word)	4	12
Data Base (MS Access)	4	12
Electronic Mail	4	14
Log-On & Virus Check	4	12
Back-up Program	4	12
Spreadsheet (i.e. MS Excel)	8	12
User Files (4 users each with 6 MB)	N/A	24
Chemical Inventory (customized COTS)	N/A	2
Training Database (customized COTS)	N/A	4
Accident Investigation & Reporting (customized COTS)	N/A	5*
Survey Recommendations (customized COTS)	N/A	4
Bar Code	640 KB	5
TOTAL	**8 MB**	**143 MB**

*Note: N/A indicates not applicable (these software packages use the RAM of the associated application software); KB indicates Kilobytes and MB indicates Megabytes. * indicates that memory was calculated by determining the total memory needed for the fields identified in figure 6.4.7-1 and multiplying by a worse case scenario of 15 accidents per week over the system life cycle.*

The amount of RAM required is the maximum of the RAM requirements and the ROM is the sum total of all ROMs. To accommodate for potential growth, systems should be developed with "the maximum amount of memory you can afford"[1] while other computer experts recommend "determining the amount of memory you think you

---

[1] Lyczak.

need and multiplying it by at least two"[1]. Requirements dictate that the system have at least two times the memory required to accommodate for future growth. Therefore, the SMITS should have a **minimum of 8 MB of RAM and 286 MB of ROM.**

---

[1] Braunstein.

7.0 MAINTENANCE CONCEPT

7.1 MAINTENANCE OVERVIEW

Maintenance is a critical element of the system life cycle which assures that the system continue to function throughout the operating life. Typically, maintenance is the most expensive aspect of system development and operation because it is the longest phase of the system life cycle and the original developers are usually not available for support. Because of this, it is essential that a strong maintenance plan is developed and implemented.

Maintenance involves preventing problems (preventive maintenance) as well as detecting and reporting problems, isolating the problem, determining the problem cause and solving the problem. The problem could be a process problem, a software problem, a hardware problem, or a combination. Because the SMITS is a computer system and is operating in a non-hostile host environment, the threat of physical damage is low. Most problems will result from user error or possibly equipment failure.

The maintenance concept for the SMITS includes: configuration management, process maintenance, and hardware maintenance and software maintenance. The system administrator plays a role which spans these prongs, and the configuration control board (CCB) must approve all modifications prior to implementation. Figure 7.1-1 depicts the maintenance overview, showing both the hierarchy and overlap.

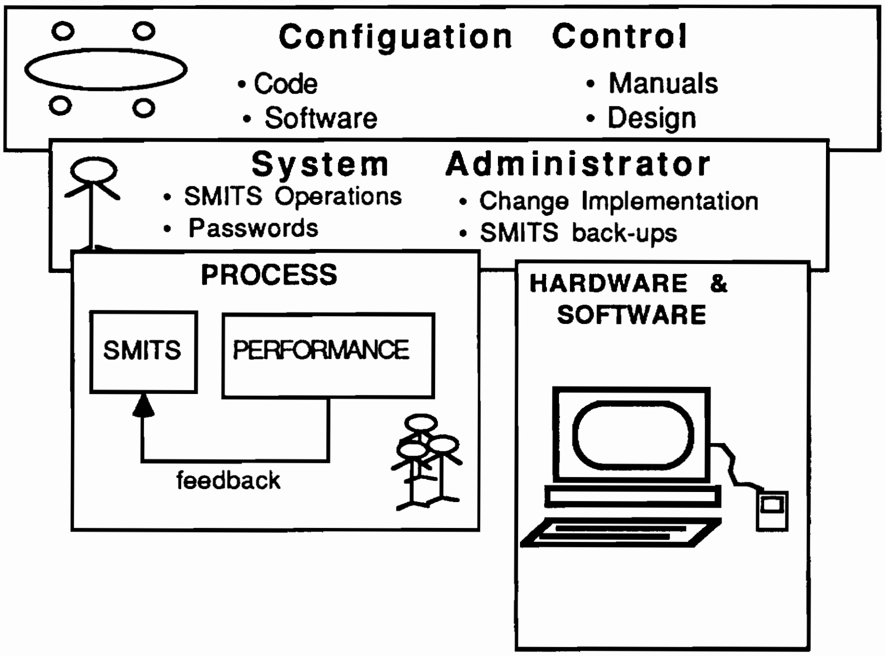


Figure 7.1-1. Maintenance Overview.

7.2 CONFIGURATION CONTROL

The final delivered and installed SMITS is considered under "control" or the "baseline". Any problem which involves changes to the baseline is subject to configuration control. Although this is a relatively small system, it is essential for the user manual(s), executable code, source code, software versions and design and test documentation to be under control, as depicted in figure 7.2-1, to prevent unauthorized changes which could damage the system or prohibit interoperability. Configuration control will reduce maintenance time and ease understanding of system in the event of system administrator transition.

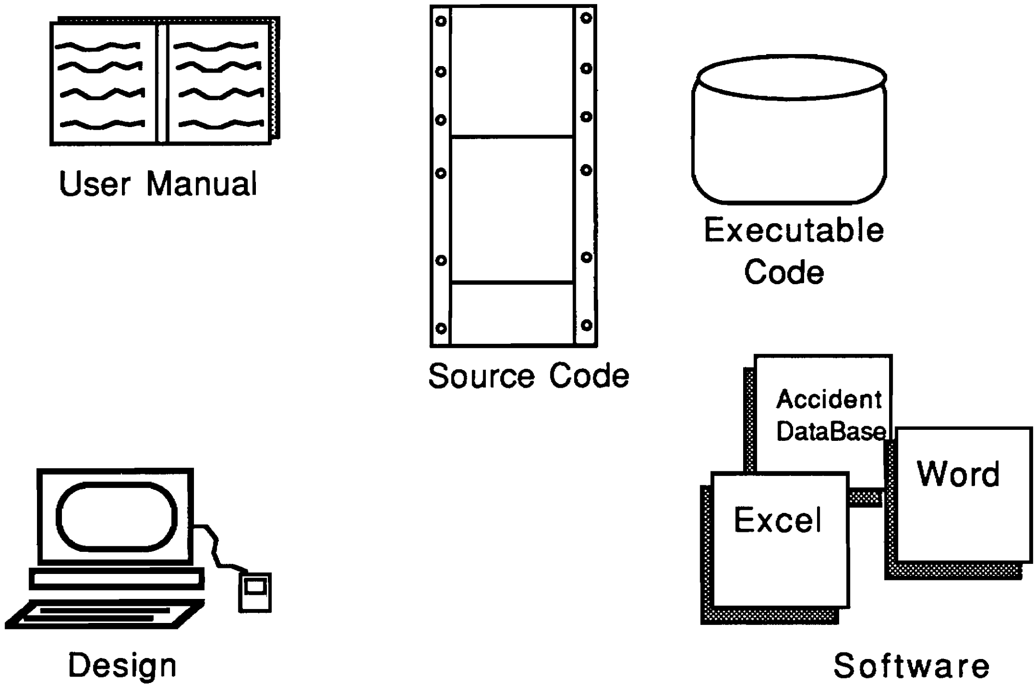


Figure 7.2-1. Items under configuration control.

The Configuration Control Board consists of the following members:

- Chief of Facilities Branch;
- Chief of Computer Engineering;
- System Administrator; and
- Suggestion/Change Proposer (non-voting).

The Chief of Facilities serves on the CCB because the system resides in his organization and funding comes from him; the Chief of Computer Engineering serves as a technical expert to challenge the change and ascertain that the change is well thought out and valid. The system administrator will present the change, potential impacts and associated cost and the board will vote on implementation. The suggestion proposer, the only non-voting member, will answer questions regarding the origin and need for the change as appropriate.

The system administrator or applicable software programmer has the ability to change the system once changes have been approved by the Configuration Control Board (CCB). The CCB will meet on an as needed basis.

7.3 PROCESS MAINTENANCE

In order to ensure that processes remain streamlined, the processes themselves as well as the system need to be periodically monitored and feedback provided to ensure system effectiveness is maintained. Employees can always find a way to improve a process[1] so once the system is in place, mechanisms need to be available for employees to suggest, recommend and improve the system. System users will be able to suggest improvements directly to the system administrator or via a suggestion box. The suggestion box will be checked weekly and the system administrator will evaluate the performance and costs trade-offs and impacts of implementation. Changes which affect the SMITS baseline will be presented to the CCB for approval.

7.4 SOFTWARE AND HARDWARE MAINTENANCE

Hardware maintenance consists of a three phased maintenance support concept. Since the system consists of a networked group of personal computers, three different approaches are required to maintain the system hardware and software; the approaches cover 1) system administrator preventive maintenance checks and services, 2) local vendor support, and 3) end item repair and replacement and are depicted in figure 7.4-1.

---

[1] Benjamin Graham, *Graham Charting Video* .

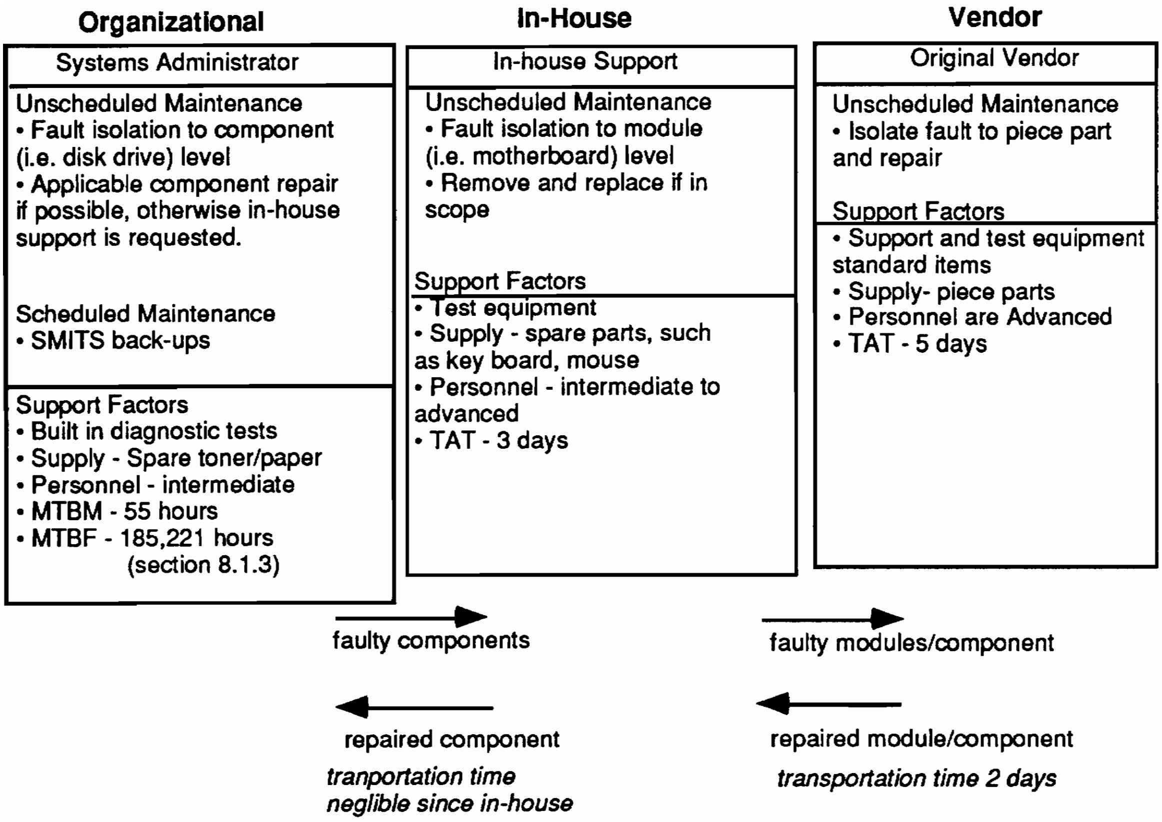


Figure 7.4-1. SMITS Maintenance concept flow.

7.4.1 Organizational Maintenance

The system administrator for the SMITS will be responsible for performing general maintenance on the system on a daily basis. This includes the actions outlined in table 7.4.1-1, where Preventive Maintenance Checks and Services is represented by the notation PMCS. Note that table 7.4.1-1 stipulates maintenance actions, the frequency of the action, and the average amount of time taken to perform the task.

TABLE 7.4.1-1 System Administrator preventive maintenance.

PMCS ACTION	FREQUENCY	TIME
Run Diagnostic	Once per Day	10 min
Perform Backups	Once per Week	143 min
Replace Paper	As Needed	5 min
Replace Toner	As Needed	10 min
Administer New Log-ons	As Needed	5 min
Implement Software Upgrades	As Needed	1 day

Note: The time for a typical back up is based on the relation:

typical back-up = 2 Megabytes data / minute[1] *[7.3-1]*

Using this relationship, and a worst case scenario of 246 bytes of data leads to the value contained in table 7.3.1-1.

Software and hardware enhancements and upgrades will be conducted for the SMITS to stay current with technology and/or incorporate new changes throughout the SMITS life-cycle. For instance, operating software will be upgraded when new versions with significant changes are released. Database changes will occur as SMITS users identify the need for modifications. All SMITS changes will be conducted outside of normal operating hours to prevent any inconvenience to the users. Upgrades will be carefully evaluated prior to implementation to asses impacts on the system and to ensure that the upgrade is cost effective.

7.4.2 Government In-House Maintenance Actions

The Government has an organization established at the site which is under contract to provide computer support to computer users throughout the site, provided that the equipment is "site-supported equipment". Site supported hardware includes IBM PCs and

---

[1] Richard T. Beerman, "MasterDat Distributed Network Backup," *LAN Technology*, (March 1993), p. 87-92.

compatibles and software includes Harvard Graphics, Word Perfect, and Lotus. In-house Government support will be available to service the SMITS system components which are site specific as required. Non-site specific software problems will be addressed directly with the software technical support. The in-house support will handle requirements upgrades, including hardware/software purchases, system relocation and other unscheduled maintenance requirements. The concept of the in-house support is to handle those maintenance requirements that cannot be serviced by the system administrator. Those problems that the in-house support cannot solve are covered by the end item repair and replacement.

The in-house maintenance team consists of hardware, software and network engineers with varying degrees of experience and expertise. Support will be assigned on an as needed basis depending upon the SMITS requirement.

7.4.3 End Item Repair and Replacement (Vendor)

In the event that a component of the SMITS system cannot be repaired by the in-house support the equipment will be returned to the manufacturer for repair if it has not been used for any classified information. If the equipment has been subjected to classified data (i.e. hard drive), then the equipment will either need to be repaired by a cleared manufacturer on site or it will need to be replaced. This type of maintenance would cover any total failure of a piece of hardware. The intent is to rarely require this level of maintenance by selecting components with high MTBF values and low MTTR values. While the component is being repaired, a replacement will be provided so that the system does not lose any functionality.

The vendors consist of the original equipment manufacturers. Service contracts will be established with these vendors.

7.5 SPARE PARTS

With the exception of printer paper and toner, spare parts for the SMITS will not be kept on-hand or in stock. Rather, the "just-in-time" policy will be followed where spares are received as needed to avoid the financial waste of stockpiling and obsolescence of parts.

8.0 REQUIREMENTS ALLOCATION

8.1 REQUIREMENTS ALLOCATION

The SMITS is broken down into different categories of parts or subsystems, and these subsystems are divided into components, as depicted in figure 8.1-1. This facilitates the allocation of requirements to different components.

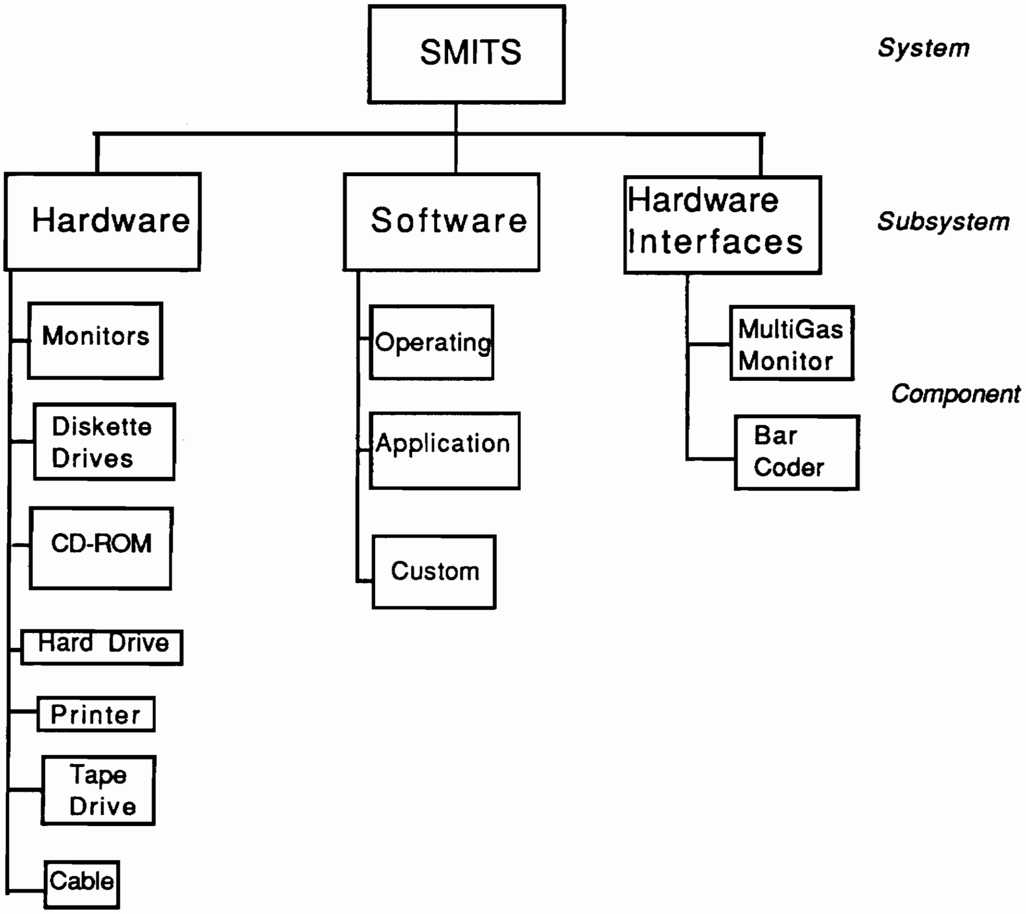


Figure 8.1-1. Hierarchy of SMITS components.

Consider, for example, the reliability of the SMITS, required to be a minimum of 85%. The reliability of SMITS depends largely on the reliability of the component parts. The SMITS consists of hardware and software. To satisfy requirements, the hardware includes the three workstations, each consisting of a 1.44 megabyte 3.5 inch diskette drive, a 15 inch flat screen crystal scan monitor, and a hard drive, a file server which doubles as a workstation, consisting of a 15 inch flat screen crystal scan monitor, a 1.44 megabyte 3.5 inch diskette drive, a 340 Megabyte hard drive, 3 CD-ROM drives (to access MSDS and EPA/OSHA regulations simultaneously), an internal tape backup drive, and a laser printer and a non-contact hand held laser scanner. Software includes the operating system, a spreadsheet package, a database application and customized databases, a word processing application, an electronic mail application, and a security application. How is the reliability of each component going to impact the overall SMITS reliability?

Typically, a Failure Mode and Effect Analysis (FMEA) is conducted during the early phases of preliminary design to identify potential problems that could result from system failure. The purpose of conducting a FMEA is to determine which components might fail, and in what way they might fail and analyze the impact of such failures on the system. However, performing a FMEA is beyond the scope of the project, although components most likely to fail are identified and a reliability analysis is performed.

8.1.1 Hardware

Hardware failures usually occur in components containing "moving parts"[1] or in static parts after delivery because "experience has indicated that the transportation, handling and storage modes are sometimes more critical from a reliability standpoint than are the conditions experienced during actual system operational use."[2] With the printer, the "projected life of the engine identifies a high level of reliability due to the fact that the electromagnetic drum is exchanged each time the toner is replaced" according to Hewlett Packard (HP) technical support and "the [HP] Division does not have Mean Time Between Failure (MTBF) data to disclose nor will they rate equipment that way in the future". For the bar code interface, no data was available on the lifetime

---

[1] Braunstein

[2] Blanchard, p. 347.

of the physical hardware. Most units will function after one drop on concrete from 3-5 feet, however, information on repeated drops is not available from manufacturers or technical representatives.

For the purposes of this reliability allocation then, the following assumptions are made:

8.1.1-1. Hard drives, diskette drives and power supplies will be the most likely components to fail after a system is installed.[1]

8.1.1-2. Bar code hand held units will not be dropped more than one time during the lifetime of the SMITS. To help ensure drops are limited to once, the hand-held scanner will be transported in a body worn holster.

8.1.2 Software

Software is a major element of this system and therefore the reliability and maintainability of the system's applications and operating system need to be considered in the design process. The definition of software reliability as defined by Blanchard is "the probability of failure-free operation of a software component or system in a specified environment for a specified time" where a failure is "an unacceptable departure of a program operation from program requirements, and a fault is the software defect that causes a failure". However, software reliability measurements are difficult to come by, if they exist at all. Software reliability metrics are determined by testing the software over an extended period of time and measuring data such as how often it fails, how many lines of code need to be changed, and the amount of repair time. Applications software personnel assert that their software is as reliable as the operating system. And operating systems people claim their software is as reliable as the hardware. So, for the purposes of reliability allocation the following assumption is made:

8.1.1-3 Software will not fail unless the hardware fails; once the hardware is fixed, the software will function properly.

---

[1] McClean

8.1.3 Reliability Analysis

Expressed mathematically, reliability, R, as a function of time, t, is:

$$R(t) = e^{-lambda * t} \qquad [1]$$

where lambda is the instantaneous failure rate. Figure 8.1.3-1 illustrates the SMITS.

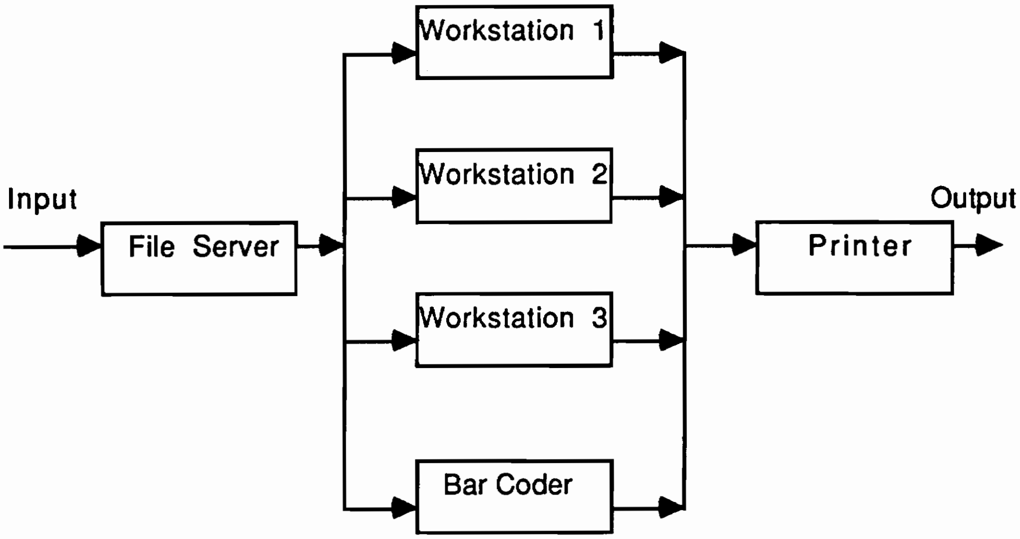


Figure 8.1.3-1. SMITS combined series-parallel network.

Each workstation is in parallel with one another and the bar coder. If any of these workstations or the bar coder stop operating, the system will still function. These components are all in series with the file server and the printer. The file server and the printer are single points of failure. Because the printer has a high reliability, it is not considered a critical component. However, the file server is a critical component; if it fails, the entire system will fail. The overall reliability of the system is found from the relation:

$$R = R_{fs} * [1-(1-R_a)(1-R_b)(1-R_c)(1-R_{bc})] * R_p \qquad [2]$$

where:

R_{fs} = reliability of the file server;
R_a = reliability of workstation 1;
R_b = reliability of workstation 2;
R_c = reliability of workstation 3;
R_{bc} = reliability of the bar coder, and

R_p = reliability of the printer.

The file server consists of several components as depicted in figure 8.1.3-2.

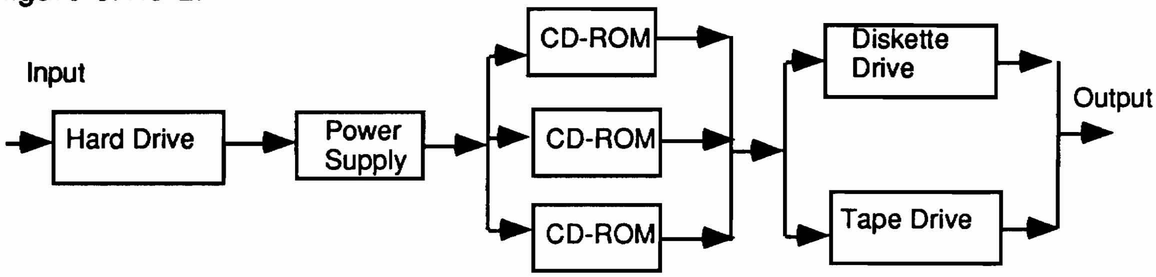


Figure 8.1.3-2. File server network.

The power supply and hard drive are single points of failure and thus are in series. As long as one CD-ROM is functioning, information will be accessible so the three drives are in parallel even though MSDS and EPA/OSHA regulations will not be simultaneously accessible if less than three are operating. The SMITS will operate regardless of whether or not the floppy drive and tape back up drive are functioning and although some functionality will be lost there are alternative means available to compensate, such as backing the system up to diskettes; however, if both fail, then SMITS will lose the capability of backing up the system. Since this is a requirement, these two components are in parallel. Analysis of figure 8.1.3-2 yields the reliability equation:

$$R_{fs} = R_{hd} * R_{cd} * [1 - (1 - R_d)(1 - R_t)] \qquad [3]$$

where:

R_{fs} = reliability of file server;
R_{hd} = reliability of hard drive on file server;
R_{cd} = reliability of CD-ROM;
R_d = reliability of diskette drive and
R_t = reliability of tape drive.

For the purposes of this analysis, the reliability of each workstation is expressed as the reliability of the power supply; the reliability of the floppy drives and hard drives on the workstation are not taken into account because for SMITS operation these functions are not essential. These features are nice to have functions which allow the workstation to operate as a standalone computer but do not impact SMITS operations. Furthermore, the reliability of the software is not taken into account because of assumption 8.1.2-1. Similarly, the reliability of the bar coder is neglected because of assumption 8.1.1-2. The reliability of the file server power supply is assumed to be one hundred percent because it will use an uninterruptable power supply (UPS) to meet requirements.

Table 8.1.3-1 shows the Mean Time Between Failure (MTBF), the failure rate (lambda) and the reliability for the critical components impacting system reliability. Reliability for each of these components is calculated using equation 1. The failure rate is the number of failures over the total mission time found by taking the inverse of the MTBF. MTBF is obtained from information obtained by vendors. The system life cycle is defined as 5 years of operating 55 hours per week which is equivalent to 14,300 hours.

Table 8.1.3-1. SMITS reliability factors.

COMPONENT	MTBF (hours)	FAILURE RATE	RELIABILITY
Power Supply	85,200[1]	.000015	.8455
Hard Drive	250,000[2]	.000004	.9444
CD-ROM	200,000[3]	.000005	.9310
Diskette Drive	150,000[4]	.000007	.9091
Tape Drive	75,000[5]	.000013	.8264

Notes:

1 - Obtained from Altex Electronics

2 - Obtained from Gateway technical support for Western Digital Caviar Hard Drive

3 - Obtained from NEC for NEC InterSect CDR-74

4 - Obtained from DynamicScan for Samsung 3.5 inch diskette drive

5 - Obtained for Jumbo Trakker 250

Evaluating equation 2 using equation 3 and the values in table 8.1.3-1 yields 92.92% file server reliability and an **overall system reliability of 92.59%**. This means that the probability or reliability of SMITS surviving for 5 operational years is 92.59 %. Figure 8.1.3- 3 allocates reliability to the components.

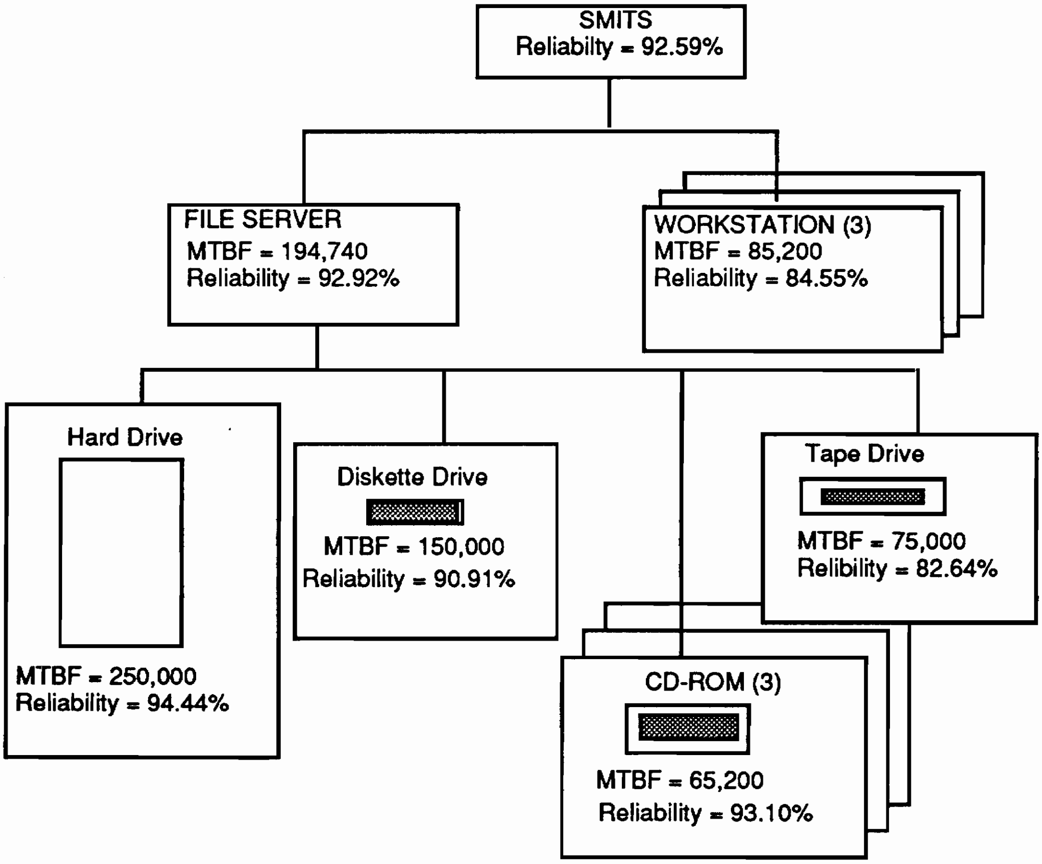


Figure 8.1.3-3. Reliability allocation.

The components with the greatest negative impact on reliability are the tape drive and the work station power supply. Although operational requirements are satisfied, selecting higher reliability parts for the SMITS design will increase system reliability. Knowing that these are the most likely to fail, in-house maintenance support can plan accordingly.

Knowing the overall system reliability, .9257, calculated in section 8.1.3 the overall system MTBF is found to be 185,221 hours by solving equation 1. The system reliability (.9257) exceeds the requirement for 85% reliability; similarly the achieved MTBF exceeds the required MTBF. Usually there is a cost trade-off associated with reliability; however, the SMITS components are standard commercially available components, no extra cost was incurred for "high reliability" parts.

9.0 LIFE CYCLE COST

9.1 COST ANALYSIS OVERVIEW

Experience has indicated that much of the cost associated with systems result from operations and support while the commitment of these costs is based upon decisions made early in the system life cycle.[1] Too often only acquisition costs are considered and as a result, projects over run or are never completed because of lack of funds. This section provides an overview of the anticipated cost of SMITS over its five year life cycle.

9.2 COST BREAKDOWN STRUCTURE (CBS)

The first step in cost analysis, after an understanding of the SMITS, is to develop a Cost Breakdown Structure (CBS) "to provide a mechanism for initial cost allocation, cost categorization, and cost monitoring and control".[2] The CBS facilitates the development of cost data and control of the development. SMITS costs are divided into three categories: research and development costs (R&D), procurement and configuration costs and operations and maintenance (O&M) support costs. Retirement and disposal costs are considered negligible, if applicable to SMITS (it is anticipated that at the end of the SMITS life cycle, the system will be up-graded, rather than disposed).

As has been discussed earlier, the SMITS design will consist of commercially available hardware and software. Customized databases will be developed using commercial application packages. Costing is based on using IBM components for the LAN file server because the file server is a single point of failure in the system (see section 8) and the in-house maintenance support consists of a cleared group of IBM employees. The file server will also function as a workstation; in addition, each of the other 3 workstations will have individual hard drives so that they can function as stand-alone PCs. Costing for software is based on Microsoft products, because they consistently receive high ratings;

---

[1] Blanchard, p. 501
[2] Blanchard, p. 512

however, market analysis indicates that Microsoft is competitively priced with Borland and other developers. The bar coder selected is a turn key system specifically designed for safety inspection and tracking.

Figure 9.2-1 contains the SMITS CBS.

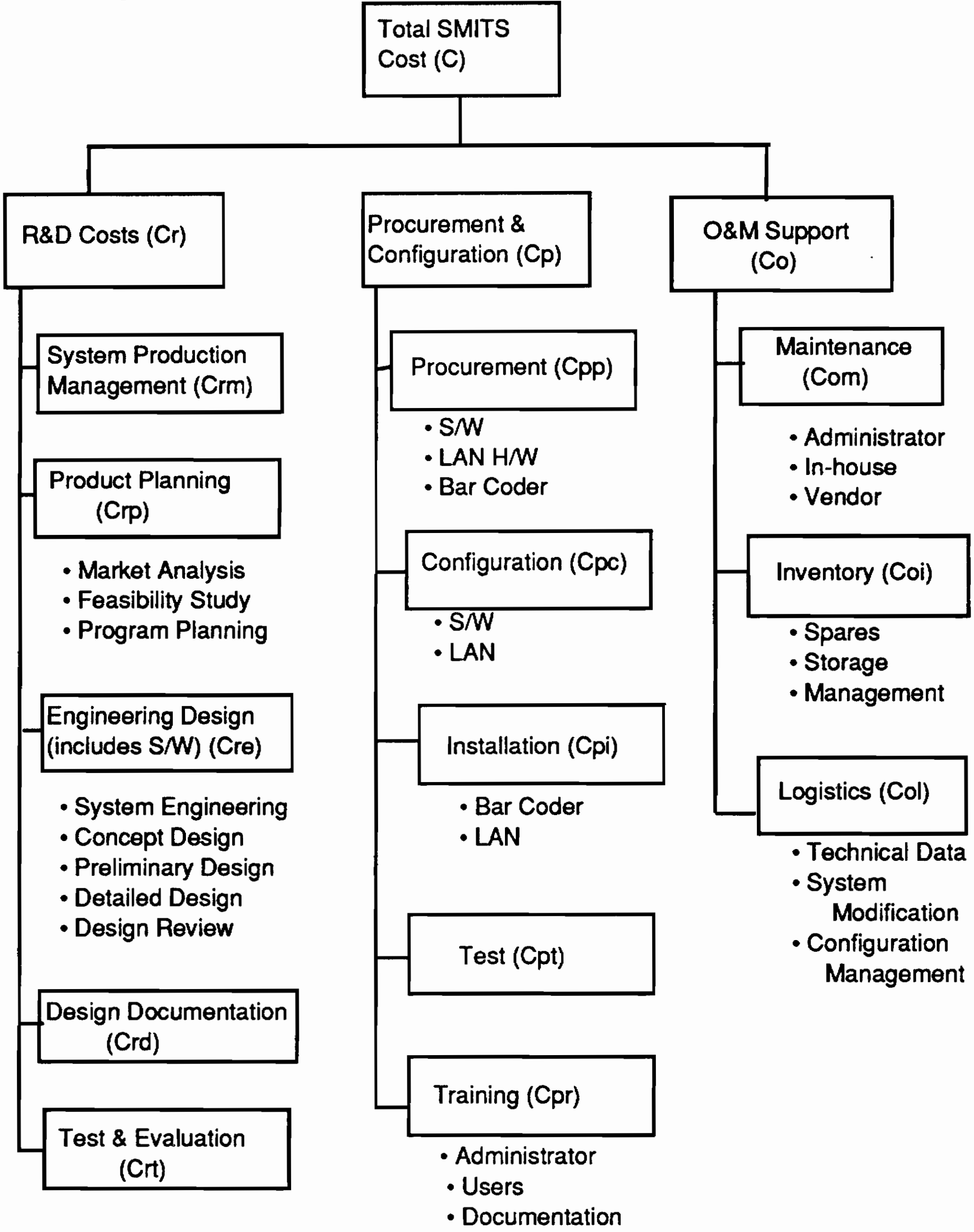


Figure 9.2-1. SMITS CBS (adapted from Blanchard, 1990).

A cost breakdown dictionary is contained in table 9.2-1, describing what each category identified in figure 9.2-1 includes.

Table 9.2-1. Cost breakdown dictionary.

ACTIVITY	DESCRIPTION
Total Cost	Includes all future costs associated with the acquisition, installation, operation and maintenance of SMITS.
R&D	Includes all costs associated with conceptual, feasibility studies, product research and actual hardware and software design.
Management	Costs associated with management of SMITS. Calculated based on premise that management would require 1 hour/week at 35$/hour for the first year and 1 hour every other week thereafter.
Production Plan	Costs of planning for SMITS. Calculated based on premise that it would require 40 hours at $25/hour.
Engineering	Costs associated with designing the system. Values obtained based on a computer engineer working for 40 hours and a system engineer working for 16 hours both at 25$/hour.
Documentation	Costs of documentation associated with design. For SMITS, this should not be too significant. Estimate based on 20 pages at $75/page.
Test &Evaluation	Cost associated with planning for and actually testing the design. Estimate based on 40 hours of testing and 40 hours of planning both at $30/hour.

Table 9.2-1. Cost breakdown dictionary. (continued)

ACTIVITY	DESCRIPTION
Procurement & Installation	Costs associated with the actual purchase and integration of SMITS components.
Procurement	Cost associated with actually purchasing SMITS components. A detailed breakdown of component costs is contained in Appendix A.
Configuration	Configuration costs cover the costs of customizing the databases to accommodate user requirements (estimated to be $1,300 in section 5) along with the costs associated with loading the software on to the hardware, estimated to require 24 hours at 20$/hour.
Installation	Refers to the costs associated with both the bar coder and the LAN. Bar code installation costs cover attaching bar code labels to extinguishers, eye washes and safety showers. This task is estimated to require 40 hours at $10/hour. LAN installation costs include setting up the workstations, printer and file server and installing the cable. This is estimated to require approximately 40 hours at $20/hour.
Test	This task covers performing an end-to-end test after the system is installed - including bar coder interfaces and Multi Gas Monitor interfaces. This task is estimated to require 8 hours at $25/hour.

Table 9.2-1. Cost breakdown dictionary (continued).

ACTIVITY	DESCRIPTION
Training	Costs associated with training include system administrator training, estimated to occur twice over the life cycle to accommodate personnel turn over at a rate of 5 days at $300/day. Additionally, users are trained, estimated at $150 per user for one day. Associated documentation is estimated to cost $1925.
O&M	Costs associated with the actual operations and maintenance of SMITS once it is installed.
Maintenance	Costs associated with system administrator, in-house and vendor maintenance. Since the MTBF exceeds system life cycle, there are no costs associated with in-house and vendor maintenance.
Inventory	Costs associated with maintaining an inventory of spare parts. At the system administrator level, no spares are maintained. At the in-house level, any spares maintained are maintained for the entire Government facility and thus cost is transparent to SMITS life cycle. In the event that this is not adequate, SMITS will rely on the JIT inventory concept. As a result, there are no costs associated with this function.
Logistics	Costs associated with technical data, system modification and configuration management. Costs for technical data based on one 2 page report per year at $100/page. System modification is estimated to cost $5,000 and is specified (see section 4) to

Table 9.2-1. Cost breakdown dictionary (continued).

ACTIVITY	DESCRIPTION
	occur once during the life cycle. Configuration management estimates are based on the premise that the board will meet 6 time per year for one hour at $50/hour.

Table 9.2-2 contains a detailed breakdown of costs associated with each item in the cost breakdown structure.

Table 9.2-2. SMITS cost allocation by program year.

Activity	**0**	**1**	**2**	**3**	**4**	**5**	**% of TOTAL**
Research & Development							
SMITS Management	910	910	910	910	910	910	5.57
Production Planning	1000						1.02
Engineering Design	1400						1.43
Design Documentation	1500						1.53
Test & Evaluation	2400						2.45
Subtotal	7210	910	910	910	910	910	12.01
Procurement & Configuration							
Procurement	43631						44.55
Software	*9075*	75	75	5075	75	75	14.75
LAN Hardware	*25081*						25.61
Bar Code	*9475*						9.67
Configuration	2600						2.65
Installation	1200						1.23
Test	200						0.20
Training	4025			1650			5.79
Administrator	*1500*			*1500*			3.06
Users	*600*			*150*			0.77
Documentation	*1925*						1.97
Subtotal	51656	75	75	6725	75	75	59.91
Operations & Maintenance							
Maintenance	3900	3900	3900	3900	1950	1950	19.91
Inventory	0	0	0	0	0	0	0.00
Logistics	500	500	500	5500	500	500	8.17
Subtotal	4400	4400	4400	9400	2450	2450	28.08
TOTAL	63266	5385	5385	17035	3435	3435	97941

Currently 100,000 dollars is allocated for developing a safety management system. Total system cost is estimated to be 97,941 dollars; this leaves less than 5% of the funds for risk mitigation. However, these numbers are somewhat deceiving. Much of the work associated with SMITS development , installation, and operation will be conducted by Government personnel. As a result, there is no "charge" to the SMITS budget for the work (i.e. installation, maintenance, design). Although there is the cost associated with the personnel not performing other tasks, it does not come out of SMITS funds.

9.3 NET PRESENT VALUE

Table 9.3-1 compares the benefits of SMITS against the cost in both cash flow today, and Net Present Value based on an interest factor of ten percent.

Table 9.3-1. Net Present Value Comparison.

	CASH FLOW			NET PRESENT VALUE	
Year, n	**Benefits**	**Costs**	**P/F,10,n**	**Benefits**	**Costs**
0	0	63,266	1	0	63266
1	0	5,385	0.9091	0	4,896
2	168,000	5,385	0.8265	138,852	4,451
3	228,000	17,035	0.7513	171,296	12,798
4	276,000	3,435	0.683	188,508	2,346
5	306,000	3,435	0.6209	189,995	2,133
TOTAL	978,000	97,941		688,652	89,889

The present equivalent analysis is founded on finding a present equivalent amount representing the difference between present equivalent savings and present equivalent costs. *The present equivalent savings or benefits for SMITS outweigh the present equivalent costs, so SMITS implementation is an extremely desirable, worthwhile venture. Within two years of operation, the SMITS benefits pay for the cost of the system over it's operating life cycle.* A detailed breakdown of how the values in table 9.3-1 were obtained is contained in Appendix C.

9.4 COST REDUCTION

Table 9.2-2 contains each activities percentage of the total system cost. A 5% reserve is not very significant. To be safe, it would be better to strive to reduce costs and increase the funds for risk management, even though system benefits outweigh costs. Table 9.2-2 shows which items contribute the most to cost. LAN hardware (H/W) is the largest contributor to cost - over 25% of the SMITS cost. One potential means of reducing costs is to purchase non-IBM workstations; compatible systems are available which cost significantly less and perform the same functions. This would impact the in-house maintenance; however, and may be more costly in the long run as the current Government policy is "any system purchased through us [the Computer Engineering Group] is maintained by us - we purchase replacements out of our budget"[1]. Another alternative is to relax the requirement for workstations to function as stand-alone systems which would eliminate the need for workstations to have hard drives.

The bar coder is very expensive. Other vendors offer bar code components at less money and for approximately half the cost of the current turn key system, a system could be procured. However, this system would not have training or consulting support ; implementation and learning curves would be extremely steep.

The OSHA/EPA CD-ROM which provides OSHA and EPA regulations on a CD-ROM database is also very expensive. A yearly subscription costs $ 5,000. For this reason, subscriptions are only purchased twice in the life cycle. However, further market search may reveal another vendor that sells the same information for less money. For example, the MSDS CD-ROM library is available from the Navy for only $75 per year to Government agencies. Perhaps there is another Government organization with the federal regulations available. This is worth additional investigation upon SMITS implementation.

9.5 LIFE CYCLE COST CONCLUSION

Although the system is costly, purchasing the system will be extremely beneficial to the Government. The system will freeing up a significant amount of time for the safety officers to implement pro-active controls rather than "fighting fires". The SMITS benefits are apparent in the savings the Government will reap ($978,000) by not having as many accidents which results in lost time and money (see table 9.3-1).

---

[1] Deaunn McLean, Computer Maintenance Engineer, interview 19 March 1993.

Additionally, the system will be able to accommodate future requirements - such as tracking hazardous waste. A recent audit of the facility by an independent party revealed that the tracking and accumulation of hazardous materials and waste is inadequate. The SMITS bar code component could be expanded to include tracking hazardous material throughout its life at the Government site.

What will happen if SMITS is **not** implemented? Although this entails a considerable amount of speculation, it is safe to assume:

1. Fire extinguishers, safety showers and eye washes will continue to go uninspected. This is acceptable, if the Government wants to risk an OSHA audit and the occurrence of an incident does which requires the use uninspected equipment which is malfunctioning. Although the likelihood of this may seem slim, it is not. During the 4 months while I was working at the Government site, we conducted a one day fire safety course. The extinguishers brought to the class had not been inspected and when the lecturer went to demonstrate, he discovered that of the five extinguishers available, four had been discharged prior to the class. Fortunately, this occurred in a class room setting and not in a real emergency.
2. Safety officers will continue to be busy filling out redundant forms and responding to incidents rather than conducting pro-active safety measures, such as site inspections.
3. Safety officers will continue to manually access information in an untimely manner, wasting time which could be spent on more productive tasks.
4. MSDSs will not be readily available. Recently, there was a chemical spill and no one could locate the MSDS. The Hazardous Response Team assumed a worst case scenario and donned full protective gear and self contained breathing apparatus, notified the nurse, and used an expensive absorbent to clean up the chemical. It turned out the chemical was not a high hazard, the Hazardous Response Team could have worn only gloves and washed the spill away with water. Approximately five

people spent 2 hours reacting the spill in an emergency mode. It all was unnecessary and cost the Government 10 working hours, the chemical absorbent and four tanks of air. This type of incident will occur again, and again, and again if the MSDS process is not improved.

5. The Government organization will continue to spend $ 1.4 million per year on accidents.

Just based on the savings associated with the decrease in the number of accidents after SMITS implementation because of more time being devoted to inspections and surveys, the SMITS pays for itself within two years.

Investing in the SMITS development is a worthwhile endeavor and while it seems like a significant amount of money, it's benefits are innumerable. The Safety Program will save the Government approximately $978,000 over five years, increase productivity, implement pro-active measures, be better equipped to deal with emergencies and the result will be a healthier, safer working environment.

10.0 CONCLUSIONS

10.1 SUMMARY

The need for an automated safety system at the Government is clearly demonstrated. A potential solution is offered which addresses the user deficiency, provides compatibility with Government maintenance processes and is technically robust. Implementation of the SMITS will improve the performance of the Safety Program, save the Government organization a significant amount of money and ultimately create a safer, healthier more productive work environment for the employees at the Government site.

10.2 RECOMMENDATIONS

Implementation of SMITS in two phases is recommended. First, the work simplification process should be applied to the current safety practices and processes to determine if they could be improved. After the processes are streamlined, the operational and maintenance requirements should be revalidated. If the same operational requirements exist, the functional analysis and design concept should be revalidated. If nothing has changed, SMITS should be implemented as proposed. However, if requirements have changed or technology has advanced, the functional analysis and resulting design concept should be readdressed and the system modified to accommodate the changes. Throughout this iterative process, performance should be measured and improved.

10.3 FUTURE STUDY

In order to optimize the SMITS implementation, further study should be given to the following areas:

- *Defining and specifying software requirements*, in general, not just in relation to the SMITS. Too often users are uncertain how to communicate their needs and requirements documents do not clearly articulate the requirement. Perhaps there is a common language missing which spans the bridge between users and developers.

Prototyping may offer one solution to ensure that the customized databases being delivered are indeed what the user wants and that the user interface is sufficiently *user harmonious*..

- *Monitoring and measuring the performance of the SMITS.* In order for the SMITS to be an effective tool, the Safety Program should implement a method to measure performance of the system and a means to improve the system.
- *Monitoring and measuring the performance of the Safety Program.* The Safety Program is more comprehensive than the SMITS and currently performance is measured only on a basis of the number of accidents per year and the percentage award fee given by the Government, which is determined somewhat arbitrarily. The Safety Program should implement additional measures to use as reference points for performance and goal setting.
- *Investigating the feasibility of interaction with a scanner.* The SMITS could interact with a scanner and MSDS and accident forms could be scanned. This was not considered as a solution because MSDS forms are not standardized and the user does not have the resources for "data intensive" work; however, the scanner might be worth pursuing in the future.
- *Investigating the potential for using the bar code system to track and status hazardous materials.* An independent auditor of the Government site recently recommended that hazardous materials and waste tracking processes be improved. If SMITS is pursued, it would be fairly easy to adapt the bar code system to this type of tracking application.

11.0 REFERENCES

1. Allais, David C. 1989. *Bar Code Symbology: Some Observations on Theory and Practice.* Lynnwood, WA: INTERMEC Corporation.

2. Beerman, Richard T. 1993. "MasterDat Distributed Network Backup." *LAN Technology*, March, p. 87-92.

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

4. Brown, David B. 1976. *Systems Analysis and Design For Safety: Safety Systems Engineering.* Englewood Cliffs: Prentice Hall.

5. Davis, William S. 1981. *Information Processing Systems.* Reading, Massachusetts: Addison-Wesley Publishing Company.

6. Derfler, Frank J., Jr. 1992. *Guide to Linking LANs.* Emeryville, CA: Ziff-Davis Press.

7. General Electric Company. 1986. *Software Engineering Handbook.* New York: McGraw-Hill Book Company.

8. Graham, Benjamin S., Jr. "Work Simplification: From Bricklayer to Microcomputer." *Templates for Information Resources Management.* p 10-13.

9. Graham, Benjamin S.,. Jr. "Information Process Charting." p 1-18, 1992.

10. Graham, Benjamin S., Jr. and Parvin S. Titus. 1979. *The Amazing Oversight: Total Participation for Productivity.* AMACOM.

11. Interview with Mark Braunstein, Program 212 Manager, General Electric M&DSO, Springfield, VA., 22 February 1993.

12. Interview (telephone) with Charlie Chilton, Manager, Environmental, Health and Safety, General Electric M&DSO, Valley Forge, PA., 25 February 1993.

13. Interview (telephone) with Chuck Fazio, Functional Administrator and Manager, General Electric AIT, Valley Forge, PA. 25 February 1993.

14. Interview with Randy Grey, Logistics Officer, General Electric M&DSO, Springfield, VA, 26 February 1993.

15. Interview (telephone) with Joseph Lyczak, Telecommunications Specialist, FDA, Washington, DC., 2 March 1993.

16. Interview (telephone) with Bill Macher, Safety Director, Department of Defense, Virginia, 11 March 1993.

17. Interview with Deaunn McLean, Computer Maintenance Engineer, General Electric M&DSO, Springfield, VA, 19 March 1993.

18. Interview with Hal Mooz, Co-Principal, Center for Systems Management, Coolfont, West Virginia, 12 February 1993.

19. Interview with David Nay, Senior Safety Engineer, General Electric M&DSO, Springfield, VA, 25 February 1993.

20. Interview with Sean Noble, Computer Services, General Electric M&DSO, Reston, VA., 26 February 1993.

21. Interview (telephone) with Matt Schaefer, Computer Sales and Engineering, Computer Ware, King of Prussia, PA., 2 March 1993.

22. Interview (telephone) with Dale J. Schillinger, Safety Director, Mallinckrodt Specialty Chemicals Company, 8 March 1993.

23. Interview with Dr. James Tomasetti, Manager, Environmental, Health and Safety, General Electric M&DSO, Springfield, VA., 27 January 1993 and 18 February 1993.

24. Interview with Greg Verveka, Project Manager, General Electric, Coolfont, West Virginia, 10 February 1993.

25. Johnson, James R. 1989. *The Software Factory: Managing Software Development and Maintenance.* Wellsley, Massachusetts: QED Information Sciences, Inc.

26. Martin, James. 1984. *An Information Manifesto.* New Jersey: Prentice-Hall Inc.

27. Mogensen, Allan. "Work Simplification - A Program of Continuous Improvement", *Industrial Engineering Handbook.* p 10-83 - 10-191.

28. Musthaler,Linda. 1993. "Send Cash." *LAN: The Local Area Network Magazine.* February, p 74-80.

29. Roy, Richard and Hal Mooz. "Government-Industry Project Management." Course presented at Coolfont, West Virginia, 1-12 February 1993.

30. Silberschatz, Abraham, James L. Peterson and Peter B. Galvin. 1992. *Operating System Concepts.* Reading MA: Addison-Wesley Publishing Company.

31. Stallings, William. 1991. *Data and Computer Communications.* New York: Macmillan Publishing Company.

32. Stallings, William. 1990. *Local Networks*. New York: Macmillan Publishing Company.

33. Thayer, Richard H. and Merlin Dorfman, eds. 1990. *System and Software Requirements Engineering*. Los Alamitos, CA: IEEE Computer Society.

34. Touby, Laurel. "Is your office a health hazard?" *SELF*, September 1992, p. 105-108.

35. Wurman, Richard Saul. 1989. *Information Anxiety*. New York: Bantam Books.

APPENDIX A. ACCIDENT INVESTIGATION AND REPORTING FORMS

ACCIDENT/INCIDENT INVESTIGATION REPORT

DATE: ______________________________

TIME: ______________________________

INDIVIDUAL: ______________________________

EXTENT OF INJURY: ______________________________

____

LOCATION: ______________________________

____

OCCURRENCE: ______________________________

____

____

____

IMMEDIATE FAILURE OR CAUSE (ACCIDENT, INCIDENT, HAZARD IDENTIFICATION):

____

____

____

____

MANAGEMENT FAILURES: ______________________________

____

____

____

____

RECOMMENDATION(S): ______________________________

____

____

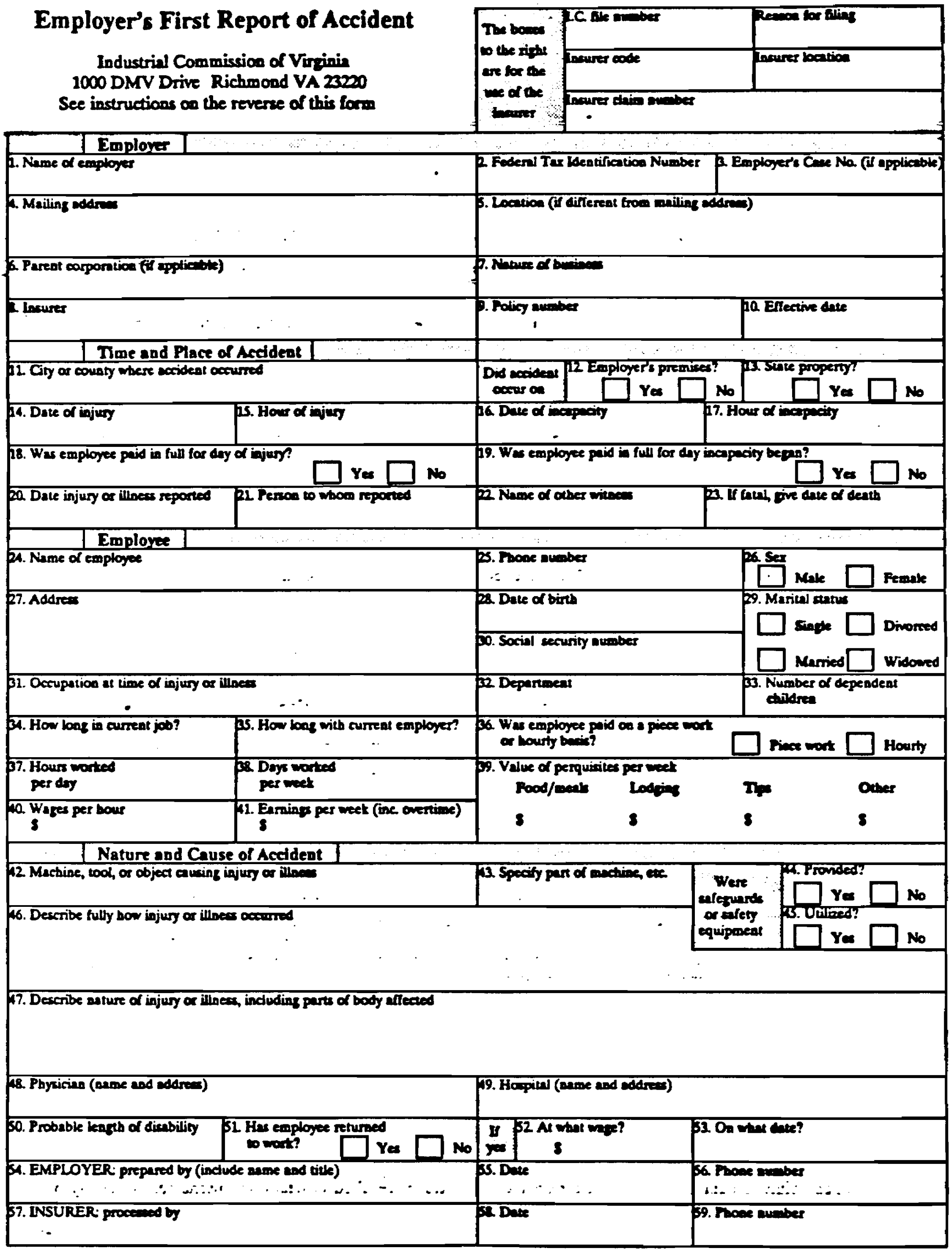
____

____

____

____

FigureA-1. Government accident investigation form.



Employer's First Report of Accident

Industrial Commission of Virginia
1000 DMV Drive Richmond VA 23220
See instructions on the reverse of this form

The boxes to the right are for the use of the insurer
I.C. file number
Reason for filing
Insurer code
Insurer location
Insurer claim number

Employer

1. Name of employer
2. Federal Tax Identification Number
3. Employer's Case No. (if applicable)
4. Mailing address
5. Location (if different from mailing address)
6. Parent corporation (if applicable)
7. Nature of business
8. Insurer
9. Policy number
10. Effective date

Time and Place of Accident

11. City or county where accident occurred

Did accident occur on
12. Employer's premises? ☐ Yes ☐ No
13. State property? ☐ Yes ☐ No

14. Date of injury
15. Hour of injury
16. Date of incapacity
17. Hour of incapacity
18. Was employee paid in full for day of injury? ☐ Yes ☐ No
19. Was employee paid in full for day incapacity began? ☐ Yes ☐ No
20. Date injury or illness reported
21. Person to whom reported
22. Name of other witness
23. If fatal, give date of death

Employee

24. Name of employee
25. Phone number
26. Sex ☐ Male ☐ Female
27. Address
28. Date of birth
29. Marital status ☐ Single ☐ Divorced ☐ Married ☐ Widowed
30. Social security number
31. Occupation at time of injury or illness
32. Department
33. Number of dependent children
34. How long in current job?
35. How long with current employer?
36. Was employee paid on a piece work or hourly basis? ☐ Piece work ☐ Hourly
37. Hours worked per day
38. Days worked per week
39. Value of perquisites per week

Food/meals	Lodging	Tips	Other
$	$	$	$

40. Wages per hour $
41. Earnings per week (inc. overtime) $

Nature and Cause of Accident

42. Machine, tool, or object causing injury or illness
43. Specify part of machine, etc.

Were safeguards or safety equipment
44. Provided? ☐ Yes ☐ No
45. Utilized? ☐ Yes ☐ No

46. Describe fully how injury or illness occurred
47. Describe nature of injury or illness, including parts of body affected
48. Physician (name and address)
49. Hospital (name and address)
50. Probable length of disability
51. Has employee returned to work? ☐ Yes ☐ No

If yes
52. At what wage? $
53. On what date?

54. EMPLOYER: prepared by (include name and title)
55. Date
56. Phone number
57. INSURER: processed by
58. Date
59. Phone number

This report is required by the Virginia Workers' Compensation Act

First Report of Accident
IC Form No. 3 (rev. 10/1/90)

Figure A-2. Virginia workers compensation form.

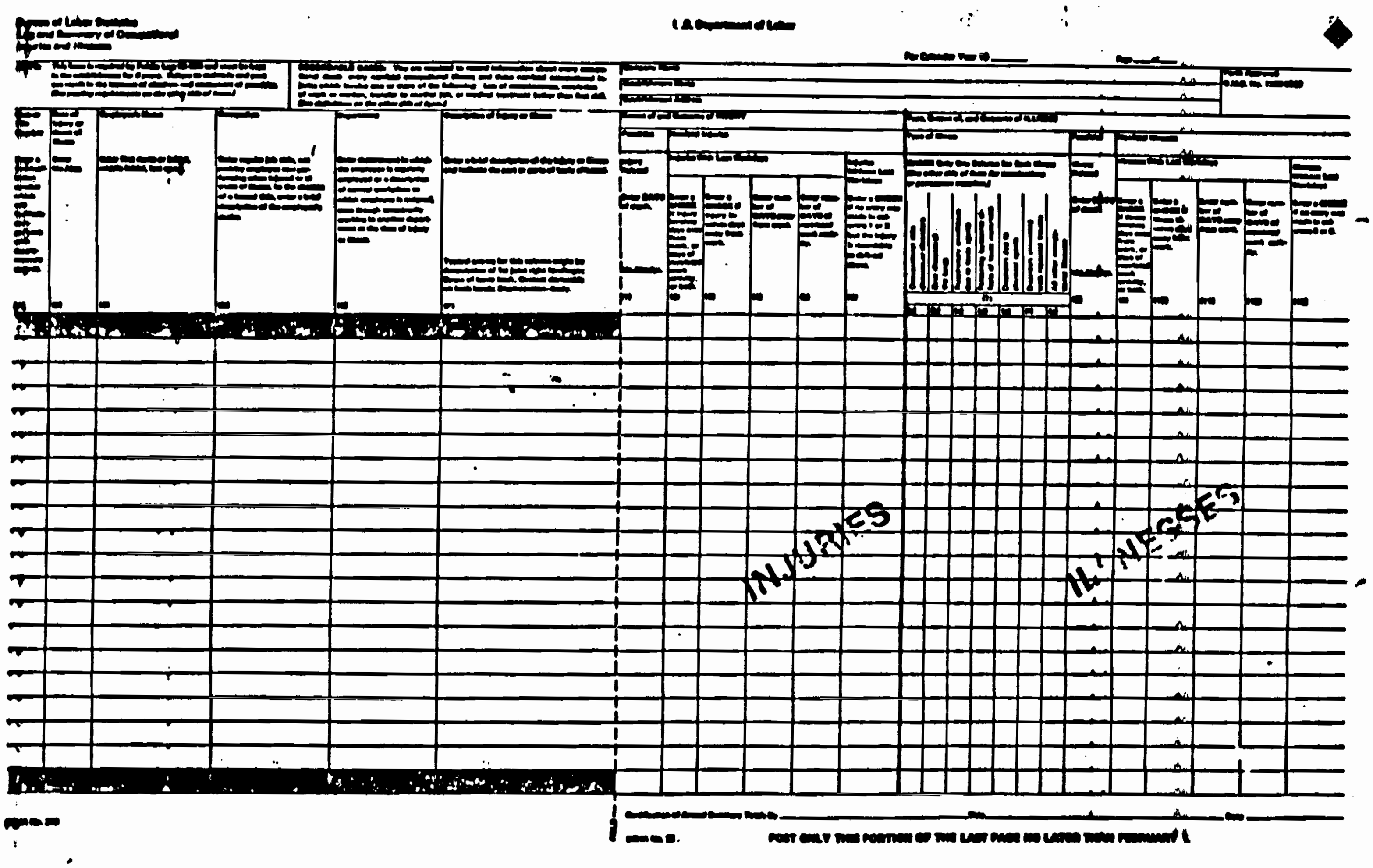


Figure A-3. OSHA required form.

APPENDIX B. DETAILED BREAKDOWN OF SMITS COMPONENT COSTS

Table B-1 divides LAN hardware, software and bar coder costs down into components so that it is clear where the costs contained in section 9 are derived from. Costs are based on vendor quotes.

Table B-1. Procurement costs.

ITEM	TOTAL COST($)
LAN Hardware	**25,081**
CD-ROM (3)	4,500
CD-ROM install kit	44
Internal Tape Drive	800
Internal Tape install kit	50
Laser Printer	2,000
Ethernet Adapter Card (4)	280
Ethernet Boot Prom (4)	120
Mouse Pad (4)	32
Mouse (4)	280
IBM DX2 *(8 MB RAM, 212 MB ROM, 3.5" diskette drive)*	3,400
NEC 21" Monitor	2,375
Workstations (3) *(Monitor, hard drive, 3.5" diskette drive)*	9,000
Cable	1,000
UPS	1,200

Table B-1. Procurement costs (continued).

ITEM	TOTAL COST($)
LAN Software	
Novell 3.11 (4)	800
Windows (4)	400
MS Word (4)	1,200
MS Excel (4)	1,200
MS Access (4)	1,200
EPA/OSHA CD-ROM *(1 initially, 1 upgrade)*	10,000
MSDS CD-ROM *(one subscription/year)*	375
Bar Coder • *PC S/W* • *Cables* • *User Manual* • *Consulting/Training* • *Microwand* • *Holster* • *Home Base*	**9,475**

APPENDIX C. SMITS BENEFITS ANALYSIS

SMITS benefits were calculated based on the number of accidents estimated to occur each year. The number of accidents which occurs is proportional to the amount of time available for proactive safety inspections and surveys. For every hour available for inspection, the risk of an accident occurring is reduced by one percent.[1] Currently there are an average of about 9 accidents per week, or 462 accidents per year and about 2.5 hours are spent on accident investigation and documentation. After SMITS implementation, investigation and documentation will only require 1.7 hours. Thus, in the first year of operation there will be the same amount of accidents but the time required to document the accidents will decrease, and this "extra" time will be available to focus on inspections and surveys. By focusing on the surveys and inspections, less accidents will occur that year, resulting in more time for inspection. This cycle will continue.

Table C-1 translates this process into the number of accidents, the time to investigate and the savings to after SMITS is implemented. The cost for each accident is based on an average 3 day absence per accident at a cost of $1000 per day, including costs associated with medical and lost work time. Prior to SMITS there were an average of 462 accidents per year, costing approximately $1.4 million. The savings calculated takes only accidents into account; however, SMITS also has the potential to help prevent OSHA and EPA fines, costs associated with chemical spills and equipment damage, among others. These savings are not factored in to the total savings as they are difficult to estimate; however, the savings from the accident costs alone make SMITS a worthwhile investment.

Table C-1. SMITS Savings

Year, n	# Accidents	#hrs per accident	#hrs available for inspeciton:	costs pos: SMITS	$saved
0	462	40	40	1386000	0
1	462	785.4	162	1386000	0
2	406	690.2	257.2	1218000	168000
3	386	656.2	291.2	1158000	228000
4	370	629	318.4	1110000	276000
5	360	612	335.4	1080000	306000
TOTAL					978000