



AD-A169 564

Final Report

on

Soldier Data Tag Study Effort

(Contract Number DATB60-84-C-0146)

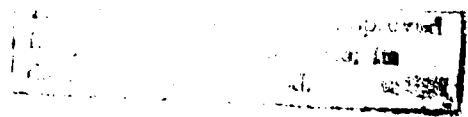
DTIC FILE COPY

Submitted to
U.S. Army Soldier Support Center
Fort Benjamin Harrison, Indiana 46216



Battelle
Columbus Division

DTIC
JUL 8 1985
[Handwritten signature]



86 7 7 207

REPORT DOCUMENTATION PAGE

HEAD INSTITUTION
DATE COMPLETION

REPORT NUMBER DA303098		REPORT ACCESSION NUMBER DA303098		REPORT NUMBER A169564	
4. TITLE (and Subtitle) SOLDIER DATA TAG			5. TYPE OF REPORT & PERIOD COVERED		
7. AUTHOR(s) BATTELLE COUMBUS LABORATORIES			6. PERFORMING ORG. REPORT NUMBER DATB60-84-C-0146		
9. PERFORMING ORGANIZATION NAME AND ADDRESS SOLDIER SUPPORT CENTER FT BEN HARRISON, IN 46216			10. PROGRAM ELEMENT PROJECT TASK AREA & WORK UNIT NUMBERS		
11. CONTROLLING OFFICE NAME AND ADDRESS ATZI-DDS (MR. OCCHIALINI)			12. REPORT DATE JUNE 1985		13. NUMBER OF PAGES 185
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office)			15. SECURITY CLASS. (of this report) Unclassified		15a. DECLASSIFICATION/DOWNGRADING SCHEDULE
16. DISTRIBUTION STATEMENT (of this Report) Approved for public release; distribution unlimited.					
17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)					
18. SUPPLEMENTARY NOTES					
19. KEY WORDS (Continue on reverse side if necessary) MICRO-CHIP PERSONNEL DATA RECORD, INTERFACE					
20. ABSTRACT (Continue on reverse side if necessary and identify by block number) The scope of the current study effort is directed at an analysis of the Soldier Data Tag System concept during both wartime and peacetime scenarios. The current study is directed primarily at Army personnel systems, medical systems, and financial systems. However, it is likely that the SDT system will have wider applications. For example, in an earlier study conducted for DoD in the logistics area, Battelle identified many feasible, cost-effective applications for portable					

BLOCK 20. (continue)

data carriers. These included inventory tags, maintenance and repair records, and manifest lists.

Data acquisition and analysis for the project was limited to that available on the SDT system concept demonstrations and emerging DoD automation systems. No detailed system design or laboratory experiments were performed.

The benefits from the SDT would be expected to lie in the areas of: improved readiness in peacetime, redundancy and backup of data for the on-line automation systems, overall improvement to the speed and accuracy of routine data entries, ability to provide a transfer data record (TDR) which replaces the error-prone paper system, and improved information processing on the battlefield.

As a result of the study, the major peacetime benefits identified for the system are primarily enhancements to the automated Army systems coming on-line. These enhancements include:

automated retrieval of data files without keyboard data entry; accessibility of data when the primary ADP system is unavailable; transportation of machine readable data to new locations in rugged format; and ability to handle the unanticipated file exchange problems that exist when a transferred soldier is diverted to a new station at the last minute.

FINAL REPORT

Submitted Under
Contract Number DATB60-84-C-0146

on

**SOLDIER DATA TAG
STUDY EFFORT**

to

U.S. Army Soldier Support Center
ATZI/DDS (Mr. Occhialini)
Fort Benjamin Harrison, IN 46216

June 10, 1985


The views, opinions, and findings contained in this document are those of the authors and should not be construed as official Department of the Army position, policy, or decision unless so designated by other official documents.

BATTELLE
Columbus Laboratories
505 King Avenue
Columbus, Ohio 43201-2693

Approved For	
By	
Date	
Initials	
Signature	
Comments	

X

A-1



AUTHORS

The research represented by this report was conducted using a multidisciplinary team at Battelle Columbus Laboratories, Columbus, Ohio, and had many contributing authors. Listed below are the major Battelle authors, organized by the project task activities.

- **Report Editing and Coordination:** Richard D. Rosen, G. Frederick Renner, Michele D. Morrison
- **System Concept Description and Analysis:** G. Frederick Renner, Barry J. Brownstein, Richard D. Rosen
- **Cost/Benefit Analysis:** Sue M. K. Garrett, Tom Martin
- **Materials Analysis:** Debbie Carter
- **Security Analysis:** Richard D. Rosen, G. Frederick Renner, Barry J. Brownstein, Richard J. Darwin
- **ADP System Compatibility Analysis:** Fred Blakeslee

Other Battelle staff members also participated in the research effort and are listed in the Acknowledgments section of this report.

EXECUTIVE SUMMARY

Since 1982 the Army has had ongoing research investigating the use of the Soldier Data Tag (SDT) System. The feasibility of the concept has been demonstrated through the use of a prototype Soldier Data Tag based on an embedded electrically erasable memory and microprocessor. The system provides a highly distributed data base which supports the potential for a high level of information transfer into areas not before possible.

The objective of the current SDT study effort is to support the development of the Army's Required Operational Capabilities (ROC) Document for the SDT System. The ROC is a concise statement of the minimal essential information necessary to initiate the Full-Scale Development Phase or Procurement of a materiel system. Battelle's study strives to support the ROC through an investigation of the issues which surround the effective design required by the Army. Specifically, these issues have been identified as:

- Security techniques for the SDT System.
- Materials considerations.
- Tag data storage technology.
- System compatibility with other Army and DoD automation.
- Cost/benefit analysis.

The scope of the current study effort is directed at an analysis of the Soldier Data Tag System concept during both wartime and peacetime scenarios. The current study is directed primarily at Army personnel systems, medical systems, and financial systems. However, through Battelle's past research and experience with portable data carrier systems, it is likely that the SDT system will have wider applications. For example, in an earlier study conducted for DoD in the logistics area, Battelle identified many feasible, cost-effective applications for portable data carriers. These included inventory tags, maintenance and repair records, and manifest lists.

Data acquisition and analysis for the project was limited to that available on the Soldier Data Tag System Concept Demonstrations and emerging

DoD automation systems. No detailed system design or laboratory experiments were performed.

The benefits from the Soldier Data Tag would be expected to lie in the areas of: (1) improved readiness in peacetime, (2) redundancy and backup of data for the on-line automation systems, (3) overall improvement to the speed and accuracy of routine data entries, (4) ability to provide a transfer data record (TDR) which replaces the error-prone paper system, and (5) improved information processing on the battlefield.

As a result of the study, the major peacetime benefits identified for the system are primarily enhancements to the automated Army systems coming on-line. These enhancements include:

- Automated retrieval of data files without keyboard data entry,
- Accessibility of data when the primary ADP system is unavailable,
- Transportation of machine readable data to new locations in rugged format, and
- Ability to handle the unanticipated file exchange problems that exist when a transferred soldier is diverted to a new station at the last minute.

Other major findings from the study are as follows:

Security Considerations

As the SDT system is targeted toward enhancing the Army's command and control system, information integrity and protection is a vital issue. In large measure, the lack of central control of the tags has both advantages and disadvantages. While the SDT system represents a new departure in the Army's distribution of information, fortunately the concept is not without its civilian parallels from which security lessons can be learned.

On the positive side, personally sensitive information is distributed to, and controlled by, the individual most interested in protecting it. The tag itself is difficult--though not impossible--to counterfeit. Also, it

potentially improves the data security of the existing centralized ADP systems by removing some of the traffic now generated by inquiries which could be satisfied by interrogating only the tag. Finally, portable data carrier technology makes available potential safeguards to penetration, such as improved methods for data encryption and personal identification.

On the negative side, the distribution of data to the individual who has the most to gain by altering it represents a temptation. Not surprisingly, the SDT system--as is the case with virtually all such systems known to man--is not intrinsically secure. It is therefore necessary to combine operational security procedures with whatever security attributes the SDT design possesses inherently, or which can be designed in. This report elaborates on the basic requirements for security and makes a preliminary assessment of the major threats, which include attacks during the design, manufacture, and distribution processes, counterfeiting, unauthorized access/alteration of tag data, and use of the tag to detect the presence of an individual on the battlefield.

Key findings are:

- It is unlikely that security in such a widely distributed and publicized system can be maintained through the use of "secret" passwords, encryption algorithms, or integrated circuit design. Instead, near-term solutions will most likely involve a combination of encryption (probably the use of public key methods of data encryption) and robust hardware architectures with some capability for electronic destruction of critical data paths.
- The SDT system changes the architecture of the involved ADP systems to a point where the number of inquiries to a central data base should be reduced. In addition, the need to keep many local copies of the same information would be reduced. It can be postulated that the use of an SDT system would increase the security of ADP systems to which it interfaces, since the volume of inquiries to that site would be reduced. Added layers of on-line security (typically not implemented because they are time consuming) could be incorporated with this reduced volume of inquiries.
- It is unlikely that an absolute security technique will be found to guarantee the protection of

militarily-critical information in the tag. This means that operational approaches will be needed to protect information on the tag needed on the battlefield and of military importance to the enemy. Additionally, attention will have to be paid to human factors so that the soldier will, in general, not want to discard the tag in combat.

- It is crucial that the threat to the SDT system be continually reevaluated, as the design of the SDT system evolves, whenever a new application is proposed or there is a change in technology or configuration of the fielded system, and periodically to reevaluate new technological tools available to potential system penetrators.

Materials Considerations

In examining candidate materials for housing the embedded electronic circuits in the SDT it was necessary to assess the advantages and disadvantages of metals and ceramics as compared to polymeric materials. In general, ceramic materials are brittle, easily fractured, and require high processing temperatures. If the material were porous it would be difficult to decontaminate and would have to be discarded upon exposure to toxic agents. Ceramic materials are also usually quite expensive.

Metals have traditionally been used as the material for the Identification Tag and have proven to be sufficient for its present use. However, metal is not suitable as a basic encasement material for the SDT. Its conductive properties would not allow it to be the substrate material for the integrated circuit. However, metal shielding at the exterior of the tag may make the SDT circuits more resistant to microwave and electromagnetic interference. Plastics differ from these other materials in the role of encasement in that they provide a combination of properties rather than extremes of a single property.

The following conclusions can be made regarding the materials considered for the tag:

- (1) Polyphenylene sulfide (PPS) and liquid crystal polymer (LCP) are the best materials for the manufacture of the SDT.
- (2) Mechanical properties for the SDT are less critical requirements than electrical, physical, and chemical properties.
- (3) Based on physical, chemical, and processing requirements; two polymeric materials, polyphenylene sulfide (PPS) and liquid crystal polymer (LCP), are viable candidates of the SDT encapsulating material.
- (4) Processing equipment life will be diminished by at least half, and utility costs will double with the use of PPS. However, estimated total unit costs for the PPS is only 4 cents more than for the LCP.

Tag Data Storage Technology

Regarding the information storage technology for the SDT, both electrically erasable memory (EEPROM) and the optical stripes appear to have attributes which satisfy the basic requirement for the tag. However, the survivability of an optical stripe in the envisioned battlefield environment is uncertain, and its level of development has not proceeded as rapidly as originally envisioned. The EEPROM has a longer track record, and has demonstrated survivability success in the prior Army experiments. If a rapid fielding of the soldier data tag system is to be accomplished, then the most logical choice is the use of the EEPROM/processing structure based on the prototype systems. It should be noted, however, that the current demonstration system still needs rigorous testing and design revisions in order to result in a design which meets the Army's overall requirements now and in the future.

System Compatibility

A major consideration with the Soldier Data Tag System is the need to interface with a variety of ADP systems. Within the Army this need is highlighted by the fact that the most existing personnel, financial, and

medical systems operate independently and on different hardware. However, the SDT concept is not restricted to the Army alone. Other service branches within DoD have data and processing requirements similar to those found in the Army. Because of the great potential from applying the SDT technology outside the Army, corresponding systems in the Navy, Air Force, and the Marines were studied from a compatible viewpoint.

Throughout DoD many new systems are now being planned and developed and some old ones are being enhanced. In addition, new hardware is being procured to replace older terminals and computers. The need for the SDT to effectively interface with these systems is obvious. But, to be most effective, SDT specifications must be incorporated into the basic design phase of these systems.

The SDT system can be made compatible with the ADP systems using software specifications such as those adopted for the prototype. It should be noted that the nature of the tag interface device functions makes its design both critical and difficult. In particular, the host interface and data manipulation functions will be driven by all applications of the SDT system, either in its original fielding or added later. Difficulties in making changes once the system has been fielded put extra emphasis on the need for flexibility, and on the importance of rigorous design review prior to implementation.

Cost Benefit Analysis

Since a detailed concept description did not exist at the outset of this study, a general SDT concept model was developed and used as the basis for the cost benefit analysis. In order to perform a sensitivity analysis on various technical aspects of the system, three SDT devices were examined. These ranged from a low unit cost, low capacity tag to a high unit cost, high capacity tag.

Enhancements to the current Army with planned automation were used as benefits. Costs were among additional resources required for the SDT system over the current Army with planned automation. The wartime measure was

qualitative. Life cycle cost techniques were used to compute the peacetime cost/benefit measure.

The wartime results indicated that a small increase in return-to-duty rates, increased speed and accuracy of casualty reporting, and the increase in correct replacement contribute to the availability of personnel on the battlefield. The command and control advantage provided by the SDT system is a result of improved information in the battlefield.

The peacetime results were also very promising. Using the low capacity SDT and the medium capacity SDT concept as an enhancement to automated system yielded a benefit over a ten-year period for medical and personnel application.

The specific conclusion based upon the cost/benefit model were:

- SDT will provide a beneficial enhancement to the planned automated system.
- The medium and/or high capacity tag will provide more expansion and, therefore, potentially more benefit than the CBA shows. Therefore, if the system application is fielded with unused capacity, it will be possible to obtain additional benefits without a major impact to the system design.

To a large degree, the future success of the SDT concept is not limited by technology; there do not appear to be any insurmountable technological barriers. On the other hand, the benefits of the Soldier Data Tag accrue from its use with other ADP systems, ranging in size from large, centralized personnel system to parachute manifest programs which can be executed on portable computers. It is the manner in which this application aspect of the tag is addressed that will have the major impact on the success of the program.

In terms of applications, the technology of the Soldier Data Tag allows the device to be fielded with only a skeleton of applications in place, as long as the tag has first been adequately designed. Early fielding would most likely involve large numbers of smaller applications, a situation that would enable a number of important payoffs to be obtained. Many of these would be in areas which were not covered by the scope of this study. The tag

design efforts necessary to make this possible should begin as soon as possible, both to speed the process of capitalizing on the potential payoffs, as well as to provide important information to designers of the large, evolving, ADP systems with which the tag should have a symbiotic relationship.

The fact that the Soldier Data Tag System operates completely off-line may lend itself to a faster fielding effort than would be possible with comparable function on-line systems. This is because, once designed, individual SDT stations can be replicated and fielded independently. In contrast, on-line system implementations require considerations for cable wireways, distance between the remote terminal and ADP interface, and total number of satellite stations, among others. These installation details complicate the fielding process.

In conclusion, **the SDT concept has a number of benefits, and addresses problems that presently could not be solved practically in any other manner.** While the limited testing done with the tag to date has answered some questions, many others remain that can only be answered by beginning an active design phase, along with further testing.

The Soldier Data Tag is an innovative concept whose technology is in-hand and represents the logical next step in distributed information systems applied to inherently off-line environments. Based on the results of our study, it is believed that a properly designed SDT system solves a basic need in military information processing in both peace and war.

Based on the findings of the study, the project team has arrived at the following recommendations:

- Because of the many benefits which can be expected from the SDT system, the design and development of the system should proceed as quickly as possible. The first applications for the system should be in "showcase" areas which are not highly integrated with emerging ADP systems in personnel, medical, and finance areas. For example, manifest functions or replacement of current meal cards are both relatively high volume applications which appear to have a high cost savings associated with them. By implementing these applications first, the Army will be able to test the reliability of the overall system and make design refinements. Once the systems are functional, the showcase attribute will

also allow potential system users from the ADP areas to evaluate the technology and identify how it can improve the efficiency of their own systems.

- The major technical issues yet to be resolved focus primarily on the hardware design and the reliability of the system. Several prototype tags and tag interface devices have been developed and limited experiments have been conducted. Prior to fielding any systems, a design review of the systems could be conducted to evaluate the current design and identify design refinements. In addition, an extensive reliability study of the current prototype tag should be undertaken to determine how well a design of this type can survive the expected environmental conditions. This study would involve testing the physical properties of the tag (effect of temperature extremes, temperature cycling, chemical agents, radiation, etc.) as well as verifying its electronic operation.

TABLE OF CONTENTS

	<u>Page</u>
DOCUMENT ORGANIZATION	xvii
Project Overview	xvii
SDT System Design Guide	xvii
System Analysis	xviii
Conclusions and Recommendations	xviii
Appendices	xviii
1.0 INTRODUCTION	1
1.1 Scope of This Study Effort	3
1.2 Research Approach	4
1.2.1 Data Collection	4
1.2.2 SDT System Concept Formulation	6
1.2.3 Data Analysis, Conclusions, Recommendations	7
1.2.4 Identification of Areas for Further Study	7
1.3 Factors Affecting This Study Effort	7
1.4 Acknowledgements	8
INTRODUCTION TO THE DESIGN GUIDE	9
2.0 SDT SYSTEM LEVEL DESIGN ISSUES	10
2.1 Statement of the SDT System Concept	10
2.1.1 SDT System Use	10
2.1.2 SDT System Components	16
2.2 Factors Influencing SDT System Design Decisions	17
2.2.1 Impacts of the Design Process	18
2.2.2 Impacts of the Fielding Process	18
2.2.3 Impacts of Supporting/Maintaining the System	19
2.3 Conclusions	21
3.0 SECURITY CONSIDERATIONS	22
3.1 The Computer Security Problem	22
3.1.1 Nature of the Environment	23
3.1.2 General Threats to Data Security	24
3.1.3 General Data Security Countermeasures	26
3.1.4 Authentication Technologies	30

TABLE OF CONTENTS
(Continued)

	<u>Page</u>
3.2 Data Security and the SDT System	35
3.2.1 SDT System Data Security Requirements	35
3.2.2 Inherent Security Characteristics of the SDT Concept	40
3.3 Potential Threats to the SDT System Security	44
3.3.1 SDT System Design and Manufacturing Sites	45
3.3.2 Hijacking of SDT System Shipments, or Large- Scale Counterfeit of SDT Systems	46
3.3.3 Unauthorized Alteration of the Tag Data	47
3.3.4 Counterfeit Tag Threat	47
3.3.5 Alteration of Tag Interface Devices	47
3.3.6 Detection of the Presence of an SDT on the Battlefield	48
3.4 Potential SDT System Penetration Countermeasures	48
3.4.1 SDT Onboard Security	49
3.4.2 Authentication Technologies	50
3.4.3 Combination Electronic Memory and Optical Memory	50
3.4.4 Data Encryption with the SDT	52
3.5 Conclusions	54
3.6 Recommendations Resulting From the Security Considerations Section	56
4.0 COMPONENT LEVEL DESIGN ISSUES	57
4.1 Information Storage Technology for the Tag	57
4.1.1 Comparison of Technologies	59
4.2 Materials Technology for the Tag	61
4.2.1 Information Analysis	61
4.2.2 Identification of Preliminary Performance Requirements	64
4.2.3 Materials Research Results	67
4.2.4 Surface Information	85
4.2.5 Conclusions	89

TABLE OF CONTENTS
(Continued)

	<u>Page</u>
4.3 Tag Interface Device Design Issues	99
4.3.1 TID Software Issues	101
4.3.2 Alternatives to Metallic Contacts	106
4.3.3 Tag Interface Device Design Issue Summary	117
4.4 Conclusions	118
4.5 Recommendations for Component Level Design Issues	119
GLOSSARY OF POLYMER/PROCESSING TERMINOLOGY	121
5.0 COST/BENEFIT ANALYSIS	123
5.0.1 Introduction to the Cost/Benefit Analysis	123
5.0.2 Scope of Cost/Benefit Analysis	124
5.0.3 Data Collection	125
5.1 Analysis Approach	126
5.1.1 Evaluation Criteria	126
5.1.2 Assumptions	126
5.1.3 Analysis Methodology	128
5.1.4 Results of Wartime Benefit Analysis	137
5.2 Results of the Peacetime Cost/Benefit Analysis	138
5.2.1 Impact on Personnel Systems	138
5.2.2 Impact on Medical Systems	139
5.2.3 Impact on Finance Systems	140
5.2.4 Combined Peacetime Cost/Benefit Results	141
5.2.5 Wartime Analysis	142
5.3 Conclusions	143
6.0 INTERACTION WITH EXISTING OR PLANNED ADP SYSTEMS	146
6.1 Compatibility Issues	146
6.1.1 Exist. and Planned ADP Systems	149
6.1.2 Soldier Data Tag Software Requirements	150
6.2 SDT Attitudes and Opinions	152
6.3 Conclusions	154
6.4 Recommendations	155

TABLE OF CONTENTS (Revised 12/31/85)
(Continued)

	<u>Page</u>
7.0 CONCLUSIONS AND RECOMMENDATIONS	175
7.1 Conclusions	175
7.1.1 Security Issues	175
7.1.2 Component Design Issues	177
7.1.3 Tag Interface Device (TID) Design Issue Summary	178
7.1.4 Cost/Benefit Analysis	179
7.1.5 ADP Compatibility Issue	181
7.2 General Recommendations	181
7.3 Identification of Areas for Further Study	184
7.3.1 Design Review of Prototype SDT Equipment	184
APPENDIX A COST/BENEFIT INFORMATION	A-1
APPENDIX B SECURITY DATA	B-1
APPENDIX C MATERIALS DATA	C-1
APPENDIX D BIBLIOGRAPHY	D-1
APPENDIX E LIST OF CONTACTS	E-1
APPENDIX F PHASE 2 - TECHNICAL EVALUATION OF CANDIDATE SYSTEMS	F-1

LIST OF TABLES

Table 2.1. General Comparison of Distributed and Centralized Data Bases	15
Table 3.1. Comparison of Personal Identification Technologies	33
Table 3.2. Summary of Security Threats and Countermeasures	53
Table 4.1. Representative Memory Price Data	60
Table 4.2. Characteristics of Candidate Polymer Classes	65

LIST OF TABLES (Revised 12/31/85)
(Continued)

	<u>Page</u>
Table 4.3. Mechanical Properties for Ryton SDT Encapsulant	66
Table 4.4. Properties and Projected Costs for Several Injection Molding Systems	69
Table 4.5. Mechanical and Physical Properties Required for SDT	71
Table 4.6. Physical Characteristics for Ryton SDT Encapsulant	75
Table 4.7. Electrical Resistivity of Polycarbonate Composites	80
Table 4.8. Printing Techniques Inappropriate for SDT Applications	90
Table 4.9. Advantages and Disadvantages of Candidate Materials	91
Table 4.10. Communication/Power Transfer Technologies	109
Table 4.11. Technology Assessment Matrix	111
Table 5.1. Intangible Costs/Benefits	130
Table 5.2. Personnel Application, Personnel Time Savings	136
Table 5.3. Dollar Cost/Benefit Results for Personnel Applications Only	139
Table 5.4. Dollar Cost/Benefit Results for Medical Applications Only	140
Table 5.5. Dollar Cost/Benefit Results Overview	141
Table 6.1. Current and Planned ADP Systems	150
Table 6.2. SDT System Compatibility	156
Table C-1. Material Cost Projection	C-2
Table C-2. Production and Equipment Requirements	C-3

LIST OF TABLES (Revised 12/31/85)
(Continued)

	<u>Page</u>
Table C-3. Projected Utilities Cost	C-4
Table C-4. Projected Labor Costs	C-5
Table C-5. Estimated Encapsulation Costs, Including Materials, Utilities, and Labor	C-6
Table C-6.	C-7

Appendix F

Table 2.1 Physical Properties of 1399X50479F (Environment)	38
Table 2.2 Physical properties of 1399X50479F (Solvents/Fuels)	42
Table 2.3 Chemical Exposure on Data Tag Prototype	44
Table 2.4 Effect of Exposure to DS2 and Bleach on Tensile Strength of Polyphenylsulfide	47
Table 2.5 Results of Exposure of the SDT to Decon Solutions	48

LIST OF FIGURES

Figure 3.1. Example of the Data Encryption Standard	28
Figure 3.2. Example of Public Key Encryption	29
Figure 4.1. Adjusting Conductive Fillers to Achieve a Semiconductive System	73
Figure 4.2. Device for Measuring Shielding Values	80
Figure 4.3. Effectiveness of EMI Shielding	81
Figure 4.4. Potential Shielding Concepts for the SDT	83
Figure 5.1. Dollar Cost and Benefits Output Matrix	129
Figure 5.2. Cost Data Sheet for O&S Equipment	131

LIST OF FIGURES (Revised 12/31/85)
(Continued)

	<u>Page</u>
Figure 5.3. Medical Data/Computation Sheet for O&S Equipment	132
Figure 5.4. Personnel Data/Computation Sheet for O&S Equipment	133
Figure 5.5. Finance Data/Computation Sheet for O&S Equipment	134
<u>Appendix F</u>	
Figure 2.1 Datakey Prototype SDT System	8
Figure 2.2 Embedded Electronics in SDT Prototype	9
Figure 2.3 Artificial Pocket Test	16
Figure 2.4 Radiograph of Datakey SDT Prototype	18
Figure 2.5 Cigarette Lighter Burn Test	20
Figure 2.6 Instron Tensile/Flexure Test	28
Figure 2.7 Gardner Wear Test	29
Figure 2.8 Izod Impact Test	30
Figure 2.9 Falling Sand Abrasion Test	32
Figure 2.10 Quartz Spring Absorption Balances	35
Figure 2.11 Thumb and Finger Grip Strength	40
Figure 2.12 Saturated HD Vapor Sorption by Data Tag Material	45
Figure 2.13 Photomicrograph of Drexler Optical Card	54
Figure 2.14 AT&T Memory Card	60
Figure 2.15 AT&T Card Reader	61
Figure 2.16 Radiograph of the AT&T Memory Card Showing the Placement of Electronics	67

DOCUMENT ORGANIZATION

The overall purpose of this report is to support the Army's Required Operational Capabilities (ROC) document by providing information which addresses critical portions of the SDT system design. In order to produce a document which is useful as a design guide, the report has been divided into four main sections: (1) background information regarding the conduct of the study, (2) a discussion of specific SDT design issues, (3) cost/benefit analysis and compatibility with other ADP systems, and (4) conclusions and recommendations. A description of the report chapters is presented below:

Project Overview

- **Introduction and Research Approach** - Describes project background, objective and scope, and data collection and analysis methodology.

SDT System Design Guide

- **SDT System Level Design Issues** - Presents the basic SDT system and describes the various system level issues concerned with basic design and operation. Discusses the relative merits of centralized and distributed data bases, and SDT configuration and distribution concepts. Also presents a brief set of tactical applications for the SDT system.
- **Security Issues** - Presents the basic security issues surrounding the design, manufacture, and usage of the SDT system. Discusses potential security threats and countermeasures.
- **Component Level Design Concepts** - Presents design technology concepts for the SDT, the interface, and the tag interface device. Specific issues include materials, communication techniques, and tag storage technology selection.

System Analysis

- **Cost/Benefit Analysis** - Using a model of the SDT system, this section examines the costs and benefits associated with the system in the personnel, medical, and financial areas.
- **ADP System Compatibility** - Discusses the compatibility of SDT system design and its compatibility with current and emerging ADP systems.

Conclusions and Recommendations

- **Conclusions** - Although concluding remarks are provided at the end of each section, this chapter summarizes the overall research findings.
- **Recommendations** - Based on the above analysis, a series of recommendations are presented which address specific design concepts, alternative technology selections, and further necessary system research.

Appendices

- In a separately bound volume, the supporting data (including calculations for the cost/benefit analysis) are provided.

For convenience, the report has been bound with tabs separating the major sections.

1.0 INTRODUCTION

For several years, the Army has had ongoing research investigating the use of the Soldier Data Tag (SDT) System. The feasibility of the concept has been demonstrated through the use of a Soldier Data Tag based on an embedded electrically erasable memory and microprocessor. The system provides a highly distributed data base, which supports the potential for a high level of information transfer into areas not before possible.

Given that the Soldier Data Tag System provides an enhanced data base, it is necessary to determine if it is a useful tool on the battlefield and in peacetime. The major issues which impact this decision are: (1) the ability to provide adequate security, (2) the ability to survive the battlefield environment, and (3) the determination of the major benefits derived from the system. It must also be realized that some of the inherent benefits that are envisioned from the use of the Soldier Data Tag System, especially in the peacetime environment, are also benefits of other Army automation efforts currently under development.

There are other benefits, however, which can only be derived from the use of a portable data carrier concept, such as the SDT. The SDT can provide information transfer to levels of the Army which cannot be attained in any other automated manner. The ability to provide a detailed medical record in the theater of operation is a prime example of this feature. One overall objective of the SDT system design is therefore to support/enhance other automatic data processing (ADP) efforts with these additional capabilities.

The benefits from the Soldier Data Tag would be expected to lie in the areas of (1) improved readiness in peacetime, (2) redundancy and backup of data for the on-line automation systems, (3) overall improvement in the speed and accuracy of routine data entries, (4) ability to provide a transfer data record (TDR) which replaces the current, error-prone paper-based system, and (5) improved information management on the battlefield. It is in these five areas that the Army perceives the greatest benefits.

The objective of the current SDT study effort is to support the development of the Army's Required Operational Capabilities (ROC) Document. The ROC is a concise statement of the minimal essential operational, technical, personnel, manpower, safety, health, human factors engineering,

training, logistic, and cost information necessary to initiate the Full-Scale Development Phase or procurement of a material system. In particular, the study strives to determine the usefulness of the SDT system through an investigation of the issues which surround the effective design required by the Army. Specifically, these issues have been identified as:

- **Security techniques for the SDT System.** What are the trade-offs with the different levels of security? This should consider the DoD requirements for security in wartime and in peacetime, design alternatives and the level of security they provide, and the relative costs and risks for the security measures.
- **Materials considerations.** Given the high degree of portability derived from the tag, it is necessary to determine methods of designing the tag for survivability in the envisioned environment. Emphasis in this area is placed in the tag encasement material.
- **Tag data storage technology.** It should be noted that this study, through the original request for proposal (RFP), is directed primarily at examining a tag concept based on an embedded microelectronic memory technique. However, it is important to note that other storage technologies may be feasible and practical for the Soldier Data Tag System. While they are addressed in this study effort, they have not received a detailed investigation due to available resource constraints. Finally, alternative communication interfaces for data transfer between the tag and tag interface device are also investigated.
- **System compatibility with other Army DoD automation.** Given the fact that there is a great deal of emphasis being placed on the development of automated data processing systems in the personnel, medical, and financial areas, it is necessary to establish whether or not the SDT System will be compatible with these systems. In addition, it is desirable to identify the potential compatibility issues which may arise in the future.
- **Cost/Benefit Analysis.** Finally, based on the above and the envisioned usage of the tag system, is the system worth the investment required?

The Soldier Data Tag Study Effort Report is intended to provide a Soldier Data Tag System Design Guide. Through this document the ramifications of various design alternatives are explained.

1.1 Scope of This Study Effort

The scope of the current study effort is directed at **an analysis of the Soldier Data Tag System concept during both wartime and peacetime scenarios**. While the system is likely to see a wide variety of applications, the current study is directed primarily at Army personnel systems, medical systems, and financial systems. Although a concept has been defined, an SDT system specification has not yet been determined, and a strict technical review of the current SDT system design is inappropriate at this time. Data acquisition and analysis was limited to that available on the prior SDT experiments and emerging DoD automation systems. No detailed system design or laboratory experiments were performed by Battelle. In addition, several of the individual task investigations were necessarily limited.

The materials investigation was limited to a study of plastic encasements only. In examining candidate materials for the SDT it was necessary to briefly assess the advantages and disadvantages of metals and ceramics as compared to polymeric materials. In general, ceramic materials are brittle, easily fractured, and require high processing temperatures. If the material is porous, it would be difficult to decontaminate and would have to be discarded upon exposure to toxic agents. Ceramic materials are also usually quite expensive. Metals have traditionally been used as the material for the military identification tag or "Dog Tag" and have proven to be sufficient for its present use. However, it is probably inappropriate for the SDT to be embedded in metal, since the encasement material would be too conductive and the SDT would not operate reliably. (Metals are, however, appropriate as an outer shield for protection against electromagnetic interference.) Plastics differ from those other materials in that they provide a combination of properties rather than extremes of a single property.

In addition, the Army's statement of work specified that **only microchip technology was to be evaluated for the data storage portion of the tag**. The rationale for this statement is based upon the Army's prior investigations of alternative technologies. However, it should be noted that, to a much lesser extent, other storage technologies were also considered in this study.

The Soldier Data Tag study effort was directed at **Army applications only**, with the exception that the Soldier Data Tag System compatibility study

necessarily examined emerging automation for all the Departments of Defense. In the cost/benefit task, original emphasis was placed on examining the large peacetime benefits that could be gained from the usage of the system, since strict cost savings can be quantified in the peacetime scenario. Wartime cost/benefits are more difficult to quantify in the medical, personnel, and financial areas. Although an explicit identification of information processing applications in the theater of operations was not specified in the original statement of work, they may represent a major justification of the system. This would be especially true if it were to be determined that sensitive data could be properly protected. For this reason, some wartime applications are described early in the report.

1.2 Research Approach

The Soldier Data Tag Study Effort was conducted using a multi-disciplinary research team at Battelle. Team members had backgrounds and experience in the following areas: DoD ADP systems, electronic systems, security technology, memory and smart card technology, microprocessor systems, polymeric materials, and defense systems analysis.

Because of Battelle's past experience in memory card and smart card products, a knowledge base of technologies, vendors, and product offerings was already available for the study. This information was utilized as necessary throughout the study.

The research approach for the study consisted of the following elements:

- 1.2.1 Data Collection.
- 1.2.2 SDT System Concept Formulation.
- 1.2.3 Data Analysis, Conclusions, Recommendations.
- 1.2.4 Identification of Issues for Further Study.

1.2.1 Data Collection

Data collection was performed through the use of site visits, literature reviews, telephone interviews, and expert interviews at Battelle.

Site visits included trips to Ft. Benjamin Harrison, and to the SIDPERS offices in Alexandria, Virginia. In addition, a site visit was made to the Data Key Corporation in Burnsville, Minnesota to gain information regarding the manufacture of the tag used in the current Army experiments.

Literature reviews were conducted for all tasks. In the system compatibility task and cost/benefit task, the literature consisted primarily of government documents. In the alternate materials and security tasks, computerized literature searches were predominantly used.

The materials task accessed two computer data bases listing plastic materials and properties: Polyprobe and Plaspec. Polyprobe is an on-line, computerized data base system which allows information to be obtained on most currently manufactured plastics. It provides over two dozen properties for over 8,100 commercially available plastics. The Plaspec data base provides processing information and various properties for over 40 families of materials.

The security task accessed the NTIS, ABI/INFORM, and INSPEC data bases over the period 1971-1984 to obtain pertinent literature. The National Technical Information Service (NTIS) is a data base containing Government-sponsored research reports. ABI/INFORM contains business-related articles, and general reports and studies available to the public. Information Services in Physics, Electrotechnology, Computers, and Control (INSPEC) is the computerized equivalent of Science Abstracts, and covers the abstracts available in scientific literature, conferences, and journals. Keywords in the areas of data security, encryption, access control, memory and smart cards, and identification systems were used to direct the search.

Another major topic of this study was to examine existing and planned ADP systems and determine specific SDT interface requirements. **For the purpose of this study, ADP systems were limited to major applications in the functional areas of Personnel, Medical, and Finance.** Information was gathered from the four service branches (Army, Navy, Air Force, and Marines) and the three components within each (Active, Reserve, National Guard) where appropriate and available. The Army identified several of its systems to be included in the study. These were VIABLE, JACS, SIDPERS, TAMMIS, and TRIMIS for the Active Army, and CAMIS for the Army Reserve and National Guard. Several initial points of contact were provided for the other service branches.

Most of the information concerning ADP compatibility and cost/benefit was obtained through telephone and face-to-face interviews with key application personnel (generally, program or project managers). Hard copy documentation was not readily available for the ADP compatibility task, usually because it contained procurement sensitive material. Detailed data on unit-level hardware configurations outside the Army was limited at best; however, general descriptions by project managers indicated that other service branches have hardware similar to the Army's.

The above interviews were not only useful for determining quantitative facts regarding the SDT system, but also in gaining a qualitative viewpoint of the attitudes and design challenges facing the SDT design team.

In addition to the above, the study team also gathered important information as a result of a recent Memory Card Conference held at Battelle-Columbus on April 10-11, 1985. The two-day conference featured manufacturers and users of memory card systems, and included the following organizations and individuals:

- Microcard
- Schlumberger
- Vericard
- Casio
- Datakey
- Transaction Technologies
- Amrix
- Integrated Health Management Systems.

1.2.2 SDT System Concept Formulation

Existing Army documents describe the prototype experiments and provide basic concepts for use of the system. However, to date there is no set of documents which fully describe the operational aspects of the SDT system in the detail necessary for the study. The revised Operation and Organizational Plan (draft May 1985) is the closest document to date. Therefore, in order to address the design issues of this study, it was necessary to establish a cohesive framework for all aspects of the system. The project team began the study by formulating a consolidated view of the system concept, based on discussions with the Army. While this framework was sufficient for the purposes of this study, it is in no way intended to be a definitive design document for the SDT system.

1.2.3 Data Analysis, Conclusions, Recommendations

The specific formats used for the data analysis are described in the various sections of this report, and the conclusions can be found at the end of each chapter. With the report written in the form of an SDT System Design Guide, individual sections are generally self-contained and do not require the reader to read the entire document. An overview of conclusions can also be found at the end of the report.

1.2.4 Identification of Areas for Further Study

Throughout the course of the study, issues were identified which were relevant to the Army's study, but which were clearly outside the original statement of work. In as much as possible with the available resources, these issues are discussed in the report. However, those issues which were considered relevant but could not be addressed are documented in the recommendations section.

1.3 Factors Affecting This Study Effort

The study was a particularly challenging project for several reasons. First, the Soldier Data Tag concept continues to evolve and, although approved in April 1984, the concept definition continues to be shaped by the Army's ADP plans. For this reason, much of the concept changed from the time the initial contract was awarded through to the present date. While this does not impact some of the task investigations, the cost/benefit analysis was particularly impacted because of a potential change in wartime applications.

Secondly, much of the data normally available in studies of this kind do not exist. For example, the compatibility study was tasked with identifying the compatibility issues with future automation systems which are not yet fully designed or fielded; tactical applications and their assumed benefits are based on battlefield scenarios only.

The results of previous small-scale experiments may not reflect full-scale implementation issues, particularly in three areas: (1) human factors (Will the soldiers use the tags?), (2) logistics (How will the tags

be distributed, used, and maintained?), and (3) security (Is the data in the system sufficiently protected?).

Finally, the study duration was short and the depth of the investigation necessarily limited to coincide with the Army's Soldier Data Tag Development Cycle.

1.4 Acknowledgements

Battelle would like to acknowledge the assistance of Mr. Chris Occhialini, the Contracting Officer's Representative, for his guidance and assistance in this effort. In addition, we would like to thank the variety of military and industrial participants whose input to this report was invaluable.

The project team would also like to acknowledge the contributions of the following Battelle staff members: Mike Bridgman, Joe Bradbury, Keith Broerman, Jim Dvorsky, Manny Luttinger, Anita Maynard, Michele Morrison, Gordon Pickett, Karen Rosen, Mark Gibson, and Charles Burkhart.

INTRODUCTION TO THE DESIGN GUIDE

This section of the report constitutes the SDT System Design Guide. It is intended to serve as a "handbook" for the Army's SDT project team during their formulation of the operational concept and subsequent design. Because of the intermediate state of the SDT concept, it is impossible at this time to recommend categorically the specific applications of various technologies. Rather, issues are identified and design impacts are discussed.

2.0 SDT SYSTEM LEVEL DESIGN ISSUES

The objective of this section is to define the Soldier Data Tag (SDT) system concept that is used for the study, and to determine the system level design issues which impact the design decisions. This chapter of the design guide focuses on SDT system design issues. It is organized as follows:

- **2.1 Statement of the SDT System Concept.** Describes the objectives, uses, and components of the system.
- **2.2 Factors influencing SDT System Design Decisions.** Describes the global factors which are relevant to design, production, fielding, and support of the system.
- **2.3 Conclusions.**

2.1 Statement of the SDT System Concept

For the purpose of this study, the concept for the SDT system was defined at a level which allowed specific discussions of various design issues (particularly security, material alternatives, and automatic data processing (ADP) system compatibility), but did not depend on specific selections of technologies nor on specific implementations. In some instances, stronger assumptions were necessary for the analysis; these are stated separately, where appropriate. Otherwise, the following concept description provides the framework for the study.

2.1.1 SDT System Use

The objectives of the SDT system can be quite succinctly stated: **provide a command and control system advantage in wartime, and an improved state of readiness in peacetime, through the use of an SDT system which provides enhanced information transfer and distribution.** Implied in this objective are requirements for storage, retrieval, and movement of information in a very flexible manner. Types of information which are expected to be first included on the tags are in the personnel, medical, and financial areas. Functions to be performed include Strength Accounting System and Personnel Accounting System, in/out processing, and medical treatment recording.

However, in order to acquire maximum benefit from the system, it must be designed in a manner which permits introduction of other application areas.

There are many requirements for the system, but most significant are the following:

- Low cost
- Battlefield ruggedness
- Easily transported
- Operable in both combat and garrison
- Compatible with other DoD information systems
- No ADP skills requirement for the SDT carrier
- No new personnel requirements.

The Soldier Data Tag System consists of the tags themselves, devices to read and write information in the tags, and software to utilize or generate the information. The tags are small, plastic devices (form factor is sized between the current metallic dog tag and the plastic identification card) which are carried or worn by the soldiers, and which are capable of storing some amount of information. Machine readability of this information is the primary issue of the system, although some human-readable information will be present on the surface of the tag.

Both the requirements and benefits expected for the Soldier Data Tag System change considerably, depending on the environment in which their use is expected. In general, three categories of environments can be considered: peacetime, transition, and wartime. During peacetime, the major uses are to provide an improved readiness and to support routine personnel, financial, medical data storage, and transportation.

Another important use of the tag is to eliminate the problems associated with "diversion" of a soldier when transferred to a new station. In Europe, where the problem seems to be most common, a high percentage of soldiers are diverted to a different destination at the last minute, while their paper (an electronic) records are shipped to the original transfer location. The soldier-carrier SDT significantly reduces the problem, since he carries his own records.

During transition from peacetime to wartime, such as predeployment and deployment situations, the tag information could prove to be the primary mechanism for maintaining records of troop position and readiness information. In a wartime situation, the tag can provide a level of information transfer which is otherwise unattainable. If the data can be properly secured, then classified orders, strength accounting, company information, etc. could be processed on the battlefield. Emergency medical information need not be secured, and its accessibility with the soldier will improve the level of medical treatment available. (However, certain medical history data could indeed require secure storage. Knowing that a soldier is a stress casualty, for example, would be very valuable information to an enemy interrogator.)

There are many DoD automation efforts currently underway which are targeted at improving the efficiency of information flow both in wartime and peacetime. The SDT system, in many ways, may represent a redundant capability because many of its functions are also intended to be performed in other on-line information systems. However, the distributed, off-line nature of the basic SDT concept allows it to provide a level of information transfer that can not be found elsewhere. Hence, if its basic data processing attributes are exploited and it is designed correctly, it will enhance--not compete with--other ADP systems.

The Army feels that the primary application for the tag will be to utilize this enhanced information system to provide improved readiness and command and control advantages. While the present SDT study effort did not explicitly call out an analysis of tactical applications for the tag, it is important to examine the general scope of applications possible in order to put the analysis of specific design issues into proper perspective. Based upon available Army documents and concept generation sessions at Battelle, a list of wartime applications of the tag include:

- (1) Strength Accounting System and Personnel Accounting System data entry for regrouping. The tag would provide a high degree of speed and reliability to this item.
- (2) Checking in replacement troops, advantages similar to those for number 1.

- (3) Store and record medical background and treatment information.
- (4) Recording access for automated stores replenishment stations. The tag would provide very fast data entry for both access to the replenishment mechanism and recording movement information about units, tanks, and mobile weapons platforms.
- (5) Control access to use and maintenance of sophisticated equipment by checking identity and ratings information stored in the tag. As more sophisticated personal identification techniques become available to the mass market at reasonable cost, it will be possible to store individual biometric traits (such as voiceprint and fingerprint) on the tag.
- (6) Casualty identification and recording. The tags could be used as data entry devices and could also provide biometric or other data useful in identification.
- (7) Courier duty. Tags could carry encrypted information. A particular block of information can be carried redundantly by several soldiers. Information may also be fragmented and the fragments carried redundantly. This information would be erased from the individual tags upon receipt.
- (8) Information scratchpad. The tag could have a small, unrestricted-use erasable area for storage of personal data or general personalization of the card. This information would be written and read at the soldier's sole request.
- (9) The tag could provide identity and other data for coded burst transmissions. This could provide a much wider variety of data entry mechanisms for Strength Accounting System and Personnel Accounting System than possible with the currently envisioned systems. Receivers would be hooked to a TACCS or similar device for consolidation and recording of the data. Each field unit would have a tag reader/transmitter. Both casualties and availability could be transmitted without voice communications by successively putting each soldier's tag into the reader and pressing an appropriate status button. The microcomputer in the transmitter would encode the information and send it burstwise. (In this scenario, it would not be necessary for soldiers to stand in line to enter data. Tags would be inserted at their convenience and transmitted later in batch mode.)

One useful way to describe the SDT System is to regard it as a maximally distributed data base. Distributed systems in general, and the SDT System in particular, facilitate local access without the need for on-line intervention by centralized systems. This characteristic of distributed systems is particularly beneficial because of their general independence from communications facilities.

Individual items can be maintained and updated very effectively with respect to bottom-up information, but top-down information requires communication facilities to accomplish updates. Although individual data items may be exposed to more threat or loss or contamination, the data base as a whole has better resilience and error correction capability. This is due to the redundancy and inherent flexibility of the data base.

It is useful to compare the overall characteristics of centralized and distributed databases with respect to individual performance measurements. As can be seen from Table 2.1, both systems have their advantages/disadvantages, and neither is clearly the best choice for any information processing situation. However, a hybrid system (such as that which would be provided by using the SDT system in cooperation with other DoD automation) would improve overall system performance if designed correctly.

Several points raised in the table warrant further discussion. For the purposes of this discussion please note that the "local" record is the one for the individual soldier involved in the transaction. Characteristics numbered 1 and 2 define the fundamental difference between centralized and distributed data bases. Access to the local record has been greatly enhanced in the distributed scheme, at the expense of access to nonlocal records. Item 3, Concurrency, involves two different operations. At the data base level, the number of simultaneous users is limited in the distributed system by the number of computers involved and in the centralized system by the processing required and number of communications channels. The second operation, access to the same record by different users, is not possible in the distributed system. In the centralized system the effect of simultaneous access can be provided, but the problems of record locking impose additional processing requirements.

TABLE 2.1. GENERAL COMPARISON OF DISTRIBUTED AND CENTRALIZED DATA BASES

Operational Characteristic	SDT	Centralized
1 Access to local record - response time - processing requirements	Immediate None	Delay Considerable
2 Access to nonlocal record	Impossible	Same as local
3 Concurrency (at data base level) (at record level)	Unlimited None	Limited Yes
4 Automated search facilities	None	Extensive
5 Communication required	Only in associated ADP systems	Always
6 Failure propagation	Local only	Global
7 Journaling, access logs	In host machine	Yes
8 Illicit access scope	Local only	Global
9 Storage capacity growth increment	Small	Large
10 Access capacity growth increment	Small	Large

Obviously, a careful match to the needs of the particular application is necessary in either case. If automated report generation with information from the entire data base is needed, then a centralized data base is indicated. This will, however, impose requirements for communications between the user and the ADP facility. Concentration of data and remote access facilities are the primary attributes of items 6 through 8, since the same advantages available to legitimate users are also available to anyone attempting to penetrate the system. (Item 6, failure propagating, refers to the phenomenon where an error at one point in the system induces subsequent errors throughout the rest of the systems. This "domino effect" is common in electronic systems.)

Economic advantages of distributed systems are shown in 8 and 9. Growth of either storage capacity or simultaneous access capacity can be accomplished in small increments. Such growth typically is possible only in large, expensive steps with centralized ADP facilities. As an example: if a large hard-disk drive is at capacity, a small increase in space may involve adding another drive. In the SDT system, storage capacity is added in increments of one tag, and access capacity by tag interface device. This allows system growth to occur very flexibly and economically.

2.1.2 SDT System Components

The SDT system actually consists of three items. First is **the tag** itself, a small, plastic-encased device which can store information. One of these is assigned to every soldier in the Army (and Army Reserve, National Guard), and is expected to be initially loaded with personnel, medical, and financial information specific to that soldier. The tag is capable of both providing and recording information in the field. Soldiers wear or carry the tag in a manner similar to the handling of the present dog tags; although the SDTs hold much more information, they are expected to be similar in both size and weight. Information stored within the tag is likely to be an abbreviated current file on the soldier. However, unlike the Military Personnel Records Jacket (MPRJ), only limited historical information is expected to be present on the tag. In addition to services, as an automated transfer data record (TDR), the SDT is also the only information source available when other ADP systems are unavailable. A limited amount of human-readable information will be placed on the surface of the tag.

The second system component is **the tag interface device**, which interfaces to a host machine from the military computer inventory on one side and a tag on the other. Information can be read from or written to the tag by the host ADP machine through the tag interface device. This does not imply on-line access, however. The tag interface device can be designed such that many local accesses take place before information is communicated in batch to a central host ADP. Just like the tag, the device is a rugged, completely fieldable item. If, as can be expected, the tag interface device is a microprocessor-based device, it will contain embedded software to communicate

with both the tag and the host machine. To keep costs to a minimum, and reliability to a maximum, the display capability of the tag interface device is probably limited to a simple indication of successful connection, e.g., indicator lights. All other display and printout devices are provided by the host.

The third system component is **operational software**, resident in the host ADP device, to utilize the information read from the tags and provide information to be stored in the tags as the various individual applications require. The host ADP systems will use their existing data bases and communications facilities as needed, but the SDT system can be expected to supplant a large burden of use from those facilities. Each application will be responsible for translating the data between the SDT system format and its own.

To facilitate various intended applications, the SDT system is likely to provide some methods for protecting the validity of data stored in the tags. These may take the form of "generic" facilities, with each application providing the specifics as appropriate for its own needs. Various methods which may be used are discussed in detail later in this report.

2.2 Factors Influencing SDT System Design Decisions

Several factors impact the SDT system design choices with respect to security, ADP compatibility, and material selection. Specifically, how the Army elects to conduct the processes of design, production, fielding, and support become major drivers in the decision process. This section addresses these global activities and their impacts. The design choices associated with these activities (security, ADP compatibility, and material selection) are discussed in the following chapters.

It should be noted that **when** the system is fielded is also a major factor in its ability to provide benefits to the Army. First, because it does provide a redundant capability in some areas when compared with other ADP projects in process, the ability to field the SDT System as early as possible allows it to provide benefits prior to the other systems. **The fact that it operates in an off-line fashion may lend itself to a faster fielding effort than that which would be possible with on-line systems.** This is because individual stations can be replicated and fielded independently.

Also, the SDT system developed has important impacts on the design choices. The system design and planning for the Soldier Data Tag System is already under way. The potential contractors and suppliers are aware of the SDT concept through ongoing discussions with the Army, and review of articles appearing in journals and popular press. All contributing technologies under consideration for use in the system are now in place. This "awareness" and availability of technology increases the probability of developing and fielding a technically successful product.

Although this system embodies a very low risk of failure, there is a potential problem of obsolescence. When the system is fielded, there may have been technologies developed which would have been very beneficial to include in the system. This problem is common to many military programs, and no quantitative method has been found which does not introduce serious technological risks. With the above in mind, it is necessary to design the initial system so that anticipated future developments in technologies (i.e., increased memory size) can be incorporated.

2.2.1 Impacts of the Design Process

To a large degree, the primary impact of the design process is the set of design choices, which are described in the next few chapters. On the other hand, the activity associated with system design has a significant impact on security: the SDT system is being conceived in public view, and its elements will be designed by people. Both of these factors must be addressed in the selection of system security techniques.

2.2.2 Impacts of the Fielding Process

The fielding process--particularly manufacturing and distribution--has important impacts on the design of the SDT system. Most of the impacts of manufacturing are addressed in the chapter on Component Level Design, however, it is important to ask that the selection of types of information to encode on the surface of the tag have interactions with the material selected and the technique by which the information is actually laid down on the tag. A description of these techniques can be found in the chapter on materials.

There are several strategies for placing surface readable information on the tag. First, the tag can contain surface information about the particular soldier, such as SSN, name, blood type, etc. Thus, it would be similar, and perhaps replace, the conventional metallic identification tag. While this is useful information, the placement of specific data on the surface ties the device to only one soldier. Since the tag is expensive (compared to a metallic tag), it may be warranted to consider a surface readable data item which would allow the tag to be reusable. A serial number, which identifies the SDT, would be one approach. A second alternative would be the placement of printed material which can be erased and reprinted at a later date.

Distribution is another matter. Although the Army has a great deal of experience with both the distribution of equipment and the handling of records, the SDT system will pose some new and perhaps unexpected issues. The tags in particular present the conflicting requirements of widespread distribution and close control. **Throughout their manufacture, shipping, and storage, the tags will have to be strictly accounted for.** The loss of a tag makes it available for attempts to penetrate or vandalize the SDT system. Assuming tags are serialized, records of serial numbers must be kept in a form which would allow fast determination of status for any given tag from the moment of manufacture on. At the time of assignment, a number of actions will take place. Records for the soldier will have to be assembled in a host ADP machine for loading into the tag. Any human-readable information specific to the soldier will also be placed on the tag, presumably using a piece of equipment other than the tag interface device. At the same time, a record showing the assignment of that tag to that soldier must be generated and inserted in the tag status data base.

2.2.3 Impacts of Supporting/Maintaining the System

Configuration control issues are more complex. Centralized data bases are usually in a constant state of change, with data formats undergoing modifications on a continuing basis. This is manageable (although expensive) because the data bases are residing in computers under close control of skilled operators. In marked contrast, the data system in the SDT will be

extremely difficult to change once fielded. An analogy can be seen with the magnetic stripe credit card. Even though its data storage scheme is extremely limited compared to the envisioned SDT, once hundreds of millions of the cards were fielded, all users of the magnetic stripe system were constrained to operate within the capabilities of the initial data structure. This is because international standards dictating the usage of the magnetic stripe had been established so that the banks, merchants, and other financial institutions could ensure compatibility of systems. The standards are more than ten years old, and did not anticipate the enormous growth of the credit card industry. Experience has shown that, while there is sufficient bulk data storage capacity to handle many of today's desired applications, the initial selection of data formats in that instance cannot support the evolution which is occurring in that industry.

Formats for data in the tag, and protocols for communicating with the tag interface device will be effectively fixed by a large and relatively unreachable installed base of tags and tag interface devices. Different application, unrelated except for their use of the SDT system, will rely on the constancy of the specifications. This puts some pressure on the initial specification effort to provide enough flexibility in the design to accommodate even applications quite different from those initially expected. Maintaining applications flexibility is one of the major goals of the design guide section in this report. Software in the host ADP systems which translates between the SDT data format and that of the specific application will have to track changes in the application. Programs which write data into tags must be carefully tested to assure that they cannot corrupt their own or other information in the tags.

There are several alternative configuration philosophies which could be employed within the tag, including:

- **All storage space in the tag is preassigned and reserved for specific applications.** This includes both the "address" within the tag, and the length of the expected data record. In this case, the tag interface device software would need to be aware of the storage formats.
- **Information in the tag is stored in an open, random-access format.** Analogous to floppy disc storage, the

individual data records would be retrievable by their record "name", and the nature of these names is standardized. However, length of individual records can now be variable, within limits of the SDT.

- **Segmented storage schemes.** In this scenario, the tag contains a multiple number of memory "segments", and these segments may be logically organized by application area (medical, financial, personnel, etc.), or level of security implemented (i.e., Segment 1 is viewable by all, Segment 2 requires password, Segment 3 requires multiple passwords, etc.), among others. This approach provides the best security, but may also limit evolutions into new application areas if the segmentation does not allow adequate memory space.

It is interesting to note that only the third configuration scheme suggests the use of an on-board processing element (such as a microprocessor).

2.3 Conclusions

The SDT concept as described in this chapter has been used as the basis from which the various technical issues in the remainder of this Design Guide were evaluated. This is particularly true with respect to the variety of peacetime and wartime applications and environments to which the system could be subjected.

It is important to note that it is difficult to examine the SDT system realistically without considering other efforts currently underway with DoD that are concerned with other forms of automation. As stated earlier, if these efforts and those of the SDT design are treated together, then the benefits of the sum will exceed those of the individual parts.

Finally, the process by which SDT is fielded is as important as the technology decisions discussed in the following chapters. When the tag is fielded, as well as how it is manufactured, distributed, and supported, will be important to its future effectiveness.

3.0 SECURITY CONSIDERATIONS

The Soldier Data Tag (SDT) system is targeted toward enhancing the Army's command and control, consequently information integrity and protection is a vital issue. In this chapter, the security requirements for the SDT system are discussed, along with analyses of potential threats and countermeasures. The chapter is organized into five sections:

- **3.1 The Computer Security Problem.** Overview of the computer security problem and countermeasures.
- **3.2 Data Security and the SDT System.** General SDT security requirements, as well as its intrinsic security characteristics.
- **3.3 Potential Threats to SDT System Security.**
- **3.4 Potential SDT System Penetration Countermeasures.** Potential countermeasures available to increase the level of SDT system security.
- **3.5 Conclusions.**
- **3.6 Recommendations.**

Finally, while the SDT system represents a new departure in the Army's distribution of information, the concept is not without its civilian parallels from which lessons can be learned. To this end, the reader is directed to the discussion of security in the electronic banking industry, which can be found in the appendix of this report. The following discussion of security in the general case of computer information systems serves to demonstrate the issue. Also discussed are approaches for dealing with the various types of threats, and the degree to which they are effective.

3.1 The Computer Security Problem

We increasingly live in a computer-based society in which information is stored in centralized files. To some extent, however, this situation predates the computer era. For example, much of the information about people and things in our society has almost always been stored in a centralized location such as the county courthouse, police station, hospital, and banking institutions.

3.1.1 Nature of the Environment

In earlier times, physical barriers, such as walls, filing cabinets, and ominous, well-constructed buildings provided adequate security by ensuring that the time, cost, and risk of obtaining information illegally was not commensurate with the value of the information obtained. The increasing electronic storage of information has, in effect, "broken down" these walls and has given rise to the problem of data security.

The subject of data security has been given considerable attention by governmental agencies, computer manufacturers, software companies, and users. Common threats to data security have been identified and effective countermeasures have been established. According to the IBM Corporation: "Data security can be defined as the protection of data from accidental or intentional disclosure to unauthorized persons and from unauthorized modifications. Techniques for security include computer hardware features, programmed routines and manual procedures, as well as the usual physical means of safeguarding the environment with security personnel, locks, keys, and badges."

It is important to note that computers have not created the data security problem, but their widespread use, together with increased demands for information-gathering activities, have compounded the problem. With computer-based information systems, it has simply become more convenient and more efficient to obtain information--regardless if the access is legal or illegal or whether it is deliberate or accidental.

There are several reasons for the fact that the data security problem has changed in the Computer Age from what it once was. These reasons are consequences of both the characteristics of the computer itself, as well as the manner in which computers are customarily used:

- **No intrinsic audit trail.** Illegal access to a computer system does not automatically leave an audit trail so that it is not always known whether or not a breach of security has occurred.
- **Shared utilization of a resource by a large number of dispersed users.** Large, on-line computer systems are normally accessed by a large number of users who may be dispersed over a wide geographic area. There are two important consequences of this situation:

- It is more difficult to oversee the potentially illicit activities of individual users.
 - The information may traverse unsecured telecommunications resources, providing yet another environment where information may be compromised without leaving a trail.
- **System complexity.** Unlike many manual systems, computer systems are complex to the point where there are no absolute **guarantees** of security. The multitude of physical paths in the hardware and logical paths in the software makes computer security a quantity that one increases or decreases one's confidence in as a function of protection measures taken, rather than one whose level of effectiveness can be measured absolutely.

Regardless of the medium involved, the crux of the data security issue lies in an individual's--and an organizations's--need for privacy. From the perspective of the individual, he or she has the right to expect that all personal data will be protected from unlawful dissemination or improper use. From the perspective of the organization, information pertaining to decision making, future plans, and current capabilities (or weaknesses) must necessarily be kept confidential to ensure organizational success. When the "organization" is the United States, as in the specific case with the SDT system, then a breach of security could well affect national security. **While the SDT system provides some fundamental security strengths relative to centralized databases, the commulative effect of information leaks from multiple penetrations of the system could become significant.**

3.1.2 General Threats to Data Security

Crime by dishonest employees accounts for more than \$10 billion annually in the private sector. More than \$1 billion of this is in the area of computer-related crimes. Statistics show that 58 percent of computer crimes are committed by operators, clerks, and other people preparing input or using output products; 35 percent involved manipulation of programs or data; and 7 percent were committed by "supertechies" who penetrated the system. Average dollar loss from this last group is approximately \$621,000 per event.

Threats to data security can be classified as "accidental" or "deliberate". Both of these are relevant to the SDT system. While much of the concern over data security relates to deliberate infiltration, the accidental disclosure of sensitive information can be equally serious. The following discussion is drawn directly from Harry Katzan, Jr.'s book entitled The Standard Data Encryption Algorithm, and addresses both aspects of the data security threat.

3.1.2.1 Accidental. An accidental compromise of data security can result from a hardware failure, a software error, a faulty systems design, or an operational mistake, such as entering the wrong information. Regardless of the reason, an accidental penetration of the data management system may make confidential information available to unauthorized persons.

3.1.2.2 Deliberate. The deliberate penetration of a data management system may take place passively or actively. Passive infiltration is similar to wiretapping and involves observing the informational traffic of a system at some point. Passive techniques apply primarily to the use of data communications facilities, but may also involve mundane activities such as inspecting waste containers for computer printouts that were generated accidentally or inappropriately. Active penetration of a data management system involves one of the following overt acts:

- The use of legitimate access to a system to obtain unauthorized information by browsing through facilities assigned to other persons.
- Obtaining information illegally by masquerading as another person through the use of identification acquired by improper means.
- The use of hardware features, software limitations, or specifically planted entry points to access restricted information. (Specifically planted entry points, also known as "trap doors", are software features that permit the security system to be bypassed.)
- The use of an open communications channel to obtain information belonging to a user by intercepting messages between the system and the user by substituting queries pertinent to the infiltrator's needs. (For

example, the infiltrator interrupts a message from the user to the system and substitutes his own query. The reply is received by the infiltrator, who returns an error message to the legitimate user.)

- Physical penetration of the system by theft of removable media, by taking over the operation of the system, or through a position associated with the computer center that permits access to the system."

3.1.3 General Data Security Countermeasures

Data security countermeasures are a set of procedural, hardware, and software elements that collectively prevent an unauthorized person from obtaining information from any data management system. Techniques include:

- Data Encryption
- Authentication Technologies.

3.1.3.1 Data Encryption. Cryptography is the art and science of making communications unintelligible to all except the intended recipients. Data encryption is a term that has been adopted referring to the application of cryptographic techniques to digital computer data. The basic idea is that the data is encyphered prior to data transmission. After being encyphered, the data is unintelligible if intercepted or stolen. After transmission or retrieval, the data is subsequently deciphered prior to processing. In the case of the SDT, sensitive data would appear in the tag in encrypted form using an algorithm such as that described below.

Although some data encryption products use proprietary algorithms to encode information, most U.S. manufacturers currently base their devices on the Data Encryption Standard (DES) developed by IBM and adopted by the National Bureau of Standards in 1976. Another approach, the public key method devised by Martin Hellman in the mid-70s, may soon also be widely adopted.

DES combines the cryptographic operations of substitution (replacing information) and transposition (scrambling the order of information) to convert plain text into cypher text. The two operations are directed by a complex algorithm that uses a variable 56-bit secret key. To decrypt a DES message the cypher text is sent through the algorithm again with the key

applied in reverse. The DES process thus requires that both the sender and recipient know the secret key. (Figure 3.1, reprinted from "High Technology Magazine", illustrates the DES Concept.)

A second encryption technique uses a "public key" system. Despite DES's widespread acceptance, the public key method has several advantages over the encryption standard. Public key systems are based on one-way, nonreversible functions which make calculations easy in one direction but very difficult in the opposite direction without certain background information. For example, it is easy to multiply two large prime numbers together to get a large composite, but very difficult to factor that composite back into its component primes.

Unlike the traditional systems that use a single key approach, public key systems use two keys--one for encryption and one for decryption. The public keys can be safely published in a directory. Once a message has been encoded, neither the sender nor an eavesdropper can decode it. Messages can only be decoded by the second (private) key, held only by its owner. (Figure 3.2, reprinted from "High Technology Magazine", illustrates the public key concept.)

The advantage of public key systems is safer and simpler key management. With DES, the system operator faces the difficult task of distributing the secret key to both sending and receiving stations. Whether delivered physically or electronically, this key could be intercepted. Because each public key user has a unique secret key that can be generated locally, no secret keys are distributed. Generated at the same time are the public keys, which pose no threat to security, since they are available to all network users. The frequency at which new keys are generated, in either secret key or public key systems, varies with the level of security desired. If key changes are frequent--daily, for instance--key management for public key systems is much easier than the private key.

Neither DES nor the public key method is foolproof. In fact, there are those who believe that weaknesses in DES might even be deliberate. Several cryptographers believe that the National Security Agency forced the adoption of a smaller key length so that the agency itself could decrypt DES messages when it felt the need.

How the Data Encryption Standard works

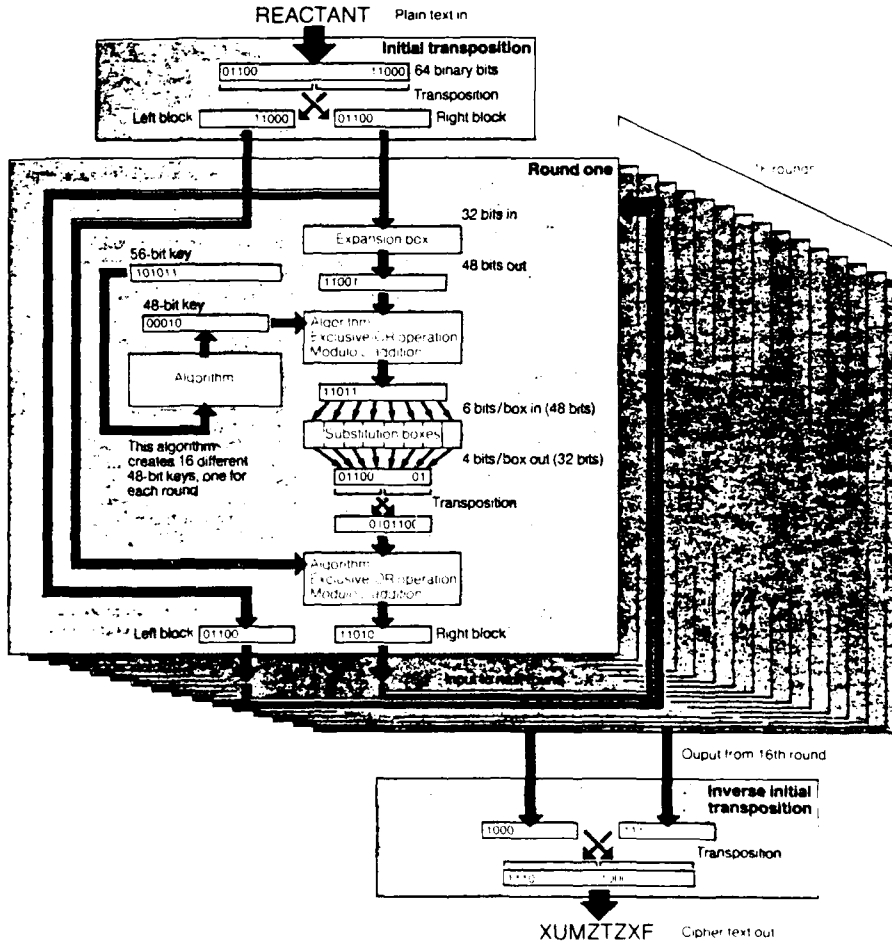
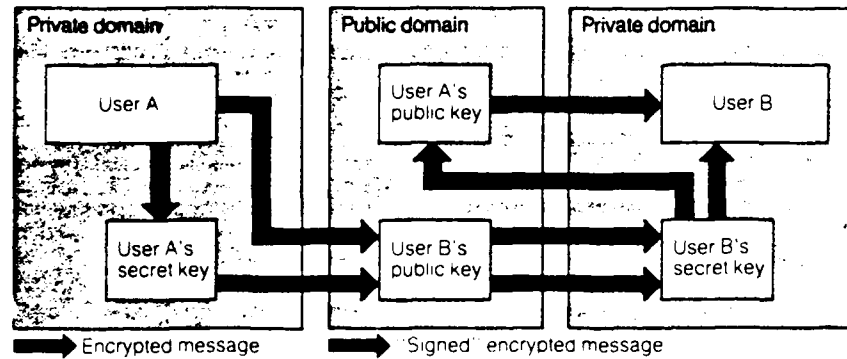


FIGURE 3.1. EXAMPLE OF THE DATA ENCRYPTION STANDARD (from "High Technology", November, 1983)

Public-key configuration



In public-key systems each user has two mathematically related keys—a public key and a secret key. Public keys are listed in a directory, but secret keys are known only to their users. User A encrypts a message with B's public key. B decodes the message with his secret key. Public-key algorithms are essentially one-way functions, so they can't be applied in reverse to decode the same message they encrypted. To "sign" a message, A encrypts the message with his secret key. B (or any other network user) can then use A's public key to decode the message, proving that A, not an imposter, sent the message. To send a private signed message to B, A encrypts the message first with his secret key, then with B's public key. Only B can decode the message, using first his secret key, then A's public key.

FIGURE 3.2. EXAMPLE OF PUBLIC KEY ENCRYPTION
(from "High Technology", November, 1983)

The security of public key systems is even less clear. When they first were developed, researchers called them "unbreakable". Yet they are inherently neither more nor less secure than conventional cryptosystems, since a weak algorithm could make any code breakable. The mathematics of public key systems have not yet been subjected to the same scrutiny of conventional cryptosystems, so the newer systems could prove to be less secure.

Given the proposed wide distribution of the SDT, it would be difficult to manage a single key system, since knowledge of the key would compromise the entire system. Since a public key system would allow each SDT to have a unique key, this encryption system should be further investigated as the preferred approach.

3.1.4 Authentication Technologies

In a widely dispersed system, it is probably as important to be able to validate prospective users as it is to protect the data by other means, such as data encryption. The problem is essentially this: How does one confirm that the individual requesting access to a data processing network is indeed who he claims to be? In the specific case of the SDT system, the problem is to insure that the holder of the tag is indeed its rightful owner. Three basic ways to do this depend on what a person "knows", what he "has", and what he "is".

A fundamental method of addressing this problem is through the use of physically secured areas for computer access. It would then be possible to perform identification check on all individuals who wished to enter the facility. This is not a realistic solution for systems such as the SDT because one of the main benefits of the system is the transportable and off-line nature of the SDT.

3.1.4.1 Passwords. Access to computers at unguarded sites has most commonly been accomplished through the use of some sort of password scheme. Here, the soldier would be required to remember a series of alphanumeric characters and use these characters whenever he inserts the SDT into the reader. Password schemes do provide some level of protection, but experience has shown that they are very easily compromised. In fact, it is very common

for one computer user to make his password known to colleagues so that they can also enter and run his files. The transference of passwords is extremely difficult to control or monitor.

Adaptations to the password scheme include the use of specialized, complex questions based on the subject's historical record. For example, at log-in time the computer system may ask for the subject's birthday, maiden or middle name, previous place of employment, etc. By asking a series of pseudo-random questions, one can establish a higher level of security than that achieved by simple passwords.

All of the variations on the password scenario involve basing the identification of the user on what he "knows". While these systems can become more and more complex, therefore providing higher levels of security, information that an individual possesses can be transferred--both consciously and subversively.

3.1.4.2 Portable Authentication Devices. The approach based on what a person "has" is typically implemented in the form of locks and keys. An electronic implementation which adds additional functions is the portable authentication device. Commercially available devices typically include onboard encryption schemes, and operate in a challenge/response sequence with software in the host ADP machine.

One typical scenario for use of an authentication device would be as follows:

- User logs onto a computer system using the usual password approach
- Once the user password security test has been passed, the host computer generates a numerical "challenge"
- Through the portable authentication device the "challenge is transformed using any of a variety of encryption techniques into the "response"
- Since the correct challenge/response pair is known to the host computer, and the response can be properly generated only by the authentication device, the host computer will permit access by only persons holding authentication devices.

Authentication device technologies parallel those used in the Soldier Data Tag itself, and thus could be implemented in conjunction with the SDT system. In this case, the challenge/response transaction could be done electronically at the machine level, avoiding both the exposure and speed problems at the display/keyboard level exchange.

3.1.4.3 Personal Identification Technologies. Another method of access control involves personal identification or verification techniques. These access control systems base their decision on the user's identification on what he "is", based upon a measurement of his biometric traits.

Many personal identification methods exist. Each of these requires the use of some specialized "reader" hardware responsible for acquiring the appropriate biometric trait. In order to be used with the SDT system, an additional device would need to be co-located with the traditional SDT reader hardware.

Each of the biometric identification analysis techniques requires that a known parameter of the individual be stored in the system. In the case of the Soldier Data Tag, the known pattern would be stored within the tag itself. **Battelle's survey of commercially available systems has shown that the amount of data required to store this data is compatible with the amount of space available in the prototype SDT.** When a soldier requested entry to an area, for example, he would identify to the system who he claimed to be. Then, his biometric feature would be measured and compared with the data on his tag. If the data correlated, he would be granted entry.

It should be noted that all personal identification techniques require that the soldier be initially registered into the system by measuring his biometric feature and storing the data on his tag. This procedure usually takes several minutes to an hour to perform.

There are six biometric parameters that are typically used in personal identification systems: fingerprint, hand geometry, palm print, signature dynamics, voiceprint, and retinal blood vessel pattern. These are briefly described below. Table 3.1 gives a comparison of the costs and storage considerations for these analysis technologies.

- **Fingerprint.** Fingerprint analysis techniques involve a scanning light source that digitizes the ridge pattern

TABLE 3.1. COMPARISON OF PERSONAL IDENTIFICATION TECHNOLOGIES

Personal Identification Technique	Current Cost for Verification Unit	Commercially Available?	Estimated Required Storage on SDT	Companies Offering Equipment
Fingerprint	\$3,500-10,000	Yes	500 bytes	Identix Fingermatrix
Hand Geometry	\$500-1,000	Yes	11 bytes	Stellar Systems Mitsubishi
Palm Print	Approximately \$1,000	Yes	50 bytes	Palmguard
Signature Dynamics	Less than \$500 (projected)	No; some expected 1st quarter '86	40 bytes	Sycon De la Rue Battelle-Geneva IBM
Voice Print	\$50,000	Yes	500-4000 bytes	Texas Instruments IBM
Retinal Blood Vessel Pattern	\$10,000	Yes	40 bytes	Eyidentify

of the individual's finger. Typically, the finger is placed against a transparent pad or into a cylindrical receptacle. The most relevant feature of the fingerprint is the "minutiae", areas of the print where two ridges join together or a single ridge ends. Approximately ten minutiae coordinates are required to characterize an individual print.

- **Hand Geometry.** This analysis technique uses the general outline characteristics of the hand to identify the individual. The measurement is performed optically, with a scanning source. Typical measurement parameters include overall hand silhouette, finger length, and finger-to-innerfinger spacing. These characteristics are not as individual as the fingerprint, and it is not unusual for two individuals in a group of 50 to have a similar hand geometry.

- **Palm Print.** The palm print is similar to a fingerprint, in that the identifying features are the lines in the center of the palm. These lines are fairly stable throughout an individual's lifetime. Palm print identifiers use a device similar to the fingerprint reader to digitize the biometric feature. The palm print is much more unique than the hand geometry, but is not as unique as the fingerprint.
- **Signature Dynamics.** While not a truly physiological parameter per se, the signature is a learned trait that can be used to identify an individual. One of the problems with the signature in general is that it is not totally repeatable, that is, signatures change with age and vary with external conditions. In order to account for these variations, signature identifiers base their analysis on the dynamics of the signature, rather than the actual appearance. Using a pressure sensitive pad, the reader measures parameters such as total signing time, pen accelerations in the "x" and "y" directions, and amount of time the pen is off the paper during the signature process.
- **Voiceprint.** These systems base the analysis on the spectral and amplitude characteristics of the voice. They usually require the individual speaking into the microphone to repeat standard phrases, such as "My name is ... ", although some systems are able to recognize an individual simply by the quality of his voice. The signal obtained via the microphone is digitized and subsequently transformed into a frequency response versus time plot. This information is compared against a known "template", and the individual is identified if the correlation between the two plots is high enough.
- **Retinal Blood Vessel Pattern.** The pattern of the blood vessels on the retinal surface of the eye are very unique to the individual, and can be used for identification. Using a low power infrared light source, a small section of the retina is scanned and the pattern is digitized. The individual is required to focus on a fixed pattern using a binocular-like instrument. This focusing procedure insures that the eye is in a known orientation during the identification scan. Some of the current researchers in this area argue that the retinal blood vessel pattern is the most unique and stable biometric feature of the human body, far surpassing even the fingerprints.

3.2 Data Security and the SDT System

As is the case with so many aspects of the analysis, the security aspects of the Soldier Data Tag System cannot be viewed effectively without looking at the entire system. From a hardware standpoint, the SDT system is not only the tag itself, but terminals, communication paths, and centralized computing resources. From an information standpoint, the system includes software, data to be protected within the system, and information which is used to authenticate an individual's right to use the system. Finally, from the standpoint of infrastructure, the approaches used in the design, manufacture, distribution, and support of the overall system have important implications on the level of security which can be realized.

The last section addressed some of the generic threats and countermeasures associated with the data security problem. In the next section, both the SDT system requirements for data security, as well as the inherent strengths and weaknesses associated with the unique nature of the SDT concept are addressed.

3.2.1 SDT System Data Security Requirements

The evolving nature of the SDT system concept makes it somewhat difficult to state absolute requirements for data security. It is clear that data security will be important, but the exact nature of the data to be protected will probably be determined by applications which are not included in the initial set. While no generically classified applications were identified to the study team, it is likely that the widespread use of the SDT would represent a resource for the future design of some classified applications.

Based on the present state of the SDT concept, the security requirements can be described by examining the three use scenarios: peacetime, deployment, and wartime.

- **Peacetime Environment.** The Soldier Data Tag System is used to support personnel, financial, and medical information systems. The soldier's tag contains detailed (and, in some cases, highly sensitive) information pertaining to these three areas.

- **Transitional Environment/Initial Deployment of Troops.** As troops are required in the theater of operation, the information within the tag will be vital to the process of rapid deployment. However, once the soldier has been deployed, the peacetime information contained within his tag could well represent a threat to national security--or the soldier--if it were to fall into enemy hands. Therefore, at the time of deployment, some reduction of data in the SDT can be assumed. As the data is extracted (and ultimately erased) from the SDT, it would be distributed electronically to the activities which require it for their operation.
- **Wartime Usage.** The amount and type of data contained on a wartime SDT has not been determined at this time. This will be controlled by the level of security provided by the system. The May 1985 Draft Operational and Organizational Plan proposes that the SDT only contain Geneva Convention and emergency medical information. No "order of battle" information will be left on the tag. If adequate security can be provided, then additional command and control can be included on the tag.

Based on these scenarios, the following SDT system security requirements can be identified:

- (1) The system should protect information whose disclosure to unauthorized personnel would constitute a violation of privacy. This information includes personnel, financial, and medical records.
- (2) The system should resist the unauthorized alteration of at least certain critical data elements in order to prevent fraudulent use or the unauthorized granting of access to resources the bearer would not normally be entitled to.
- (3) The system should be resistant to pathological penetration. That is, the extensive study of a set of tags and/or terminals should not result in the compromise of the total system.
- (4) Since the SDT system could play a very important role in a deployment operation, the system should be designed and operated so that the effect of illicit modules of hardware and/or software would not compromise the operation.
- (5) It should be assumed that terminals, tags, and valid authorization passwords (or their equivalent) will

fall into the hands of a potential adversary. Given this assumption, the system should be designed so that:

- (a) the data carried by an individual soldier in a wartime setting will not result in useful intelligence data, such as a soldier's skill set or unit
 - (b) the tag could not be used by an individual adversary to gain access to any resources or facilities which could adversely impact military operations.
- (6) The system should be designed and used so that it is likely that individual soldiers will trust the tag to the point where they will feel safe carrying it in wartime. It should be noted that this issue involves human factors at least as much as it involves technology and its application.

In addition to the general security requirements listed above, several regulatory factors are also likely to effect the SDT system design. These are:

- Privacy Act of 1974
- Federal Regulation 360-360 on Physical Security
- Geneva Convention Statutes.

The above three areas have sparked many discussions by the intended user community of the SDT system. The subject of these conversations has largely focused on how the SDT concept impacts the above items, and vice versa. Presented below is a brief discussion of these issues.

3.2.1.1 Privacy Act of 1974. The portable, distributed data base capabilities of devices like the soldier data tag and the financial smart card have often conjured up pictures of "big brother syndrome" in the minds of some potential users. For this reason, some concern has been expressed regarding whether these systems compromise an individual's right to privacy.

The Privacy Act of 1974 relates to the collection of personal data, as it impacts computer data security. The Act involves the right of individuals to control or influence what information about them may be collected

and stored, by whom, for what specific reasons, and to whom that information may then be disclosed.

The Privacy Act also covers the right of individuals to know if information about them has been compiled, and if the said information is correct and complete. Furthermore, the individual has the right to challenge the accuracy of the information.

Three aspects of the Act should be noted:

- Each agency must maintain steps to insure the security and confidentiality of the information, and must protect against anticipated threats which could result in harm, embarrassment, inconvenience, and unfairness, to the individual on whom the information is disclosed
- Each agency must record disclosures of certain types of information for auditing purposes
- Each agency must establish rules of conduct for persons involved in the design, operation, and maintenance of any system involving personal data.

Just as the current paper-based and automated files on the soldier must comply with the Privacy Act, so must the proposed SDT system. In many ways, the SDT is planned to be an abbreviated or exact replacement for existing paper documents and their associated processing, and therefore, would comply with the Act.

The potential problem that may arise through widespread use of the SDT stems from the fact that the SDT is intended to carry multiple data records for many different application areas. These various system users are not always authorized to view all the data in the tag. The following items may be relevant during the upcoming detailed design of the SDT system.

- The memory within the tag must be segmented in such a way as to discourage the possibility of unauthorized reading of certain data segments. Each application must be keyed to specific data areas.
- An audit trail of SDT uses may be required.
- The physical act of the soldier placing his tag into the reader could, in a broad sense, represent sufficient authorization for the system to access the tag data. However, an argument to this statement could be made that the soldier is not actually aware that all of

the data is being accessed at the specific time. Hence, it may be necessary for the soldier to "see" the data transaction take place based on his authorization.

It should be noted that the privacy issues associated with the SDT system are not substantially different from any automated database. Understanding the implications of the Act, and designing sufficient physical and data protection at the outset should eliminate any problem in complying with the regulation.

3.2.1.2 Regulation 360-360 on Physical Security of Computer Automation Systems. This set of regulations primarily addresses the physical security requirements of data processing facilities. Restricted access areas, proper auditing procedures, and protection from fire, flood, and other disasters are specified in the document.

This regulation is relevant to the SDT system operation primarily in terms of protecting the SDT central facilities. Tag Interface Devices that are part of portable systems must also be physically protected to guard against theft, tampering, and vandalism.

One of the most important areas of the SDT system that must be protected is the storage, initialization, and distribution areas for the tags. An analogy can be drawn here to commercial credit card initialization--one of the most overlooked functions from a security systems standpoint. Many of the successful system attacks on credit cards start at this point, with large volumes of fraudulently issued cards being generated.

SDT's will likely be physically stored, initialized, and distributed at many geographical locations. Systems designers can draw upon the experiences of the financial industries to provide a secure methodology for this procedure. (See Security Appendix for a detailed discussion of financial system security.)

3.2.1.3 Geneva Convention Statutes. Article 17 of the Third Geneva Convention stipulates the minimum amount of information that must be provided by a prisoner of war. The soldier's surname, given name, branch of service, rank, service number, and date of birth, are to be provided. A separate article specifies the ID tag which the soldier is required to carry. It is to

contain the information listed above, with the option of adding a signature or fingerprint. Soldiers are required to show, but not to surrender, the ID tag to their captors.

Due to the fact that data security in the tag may not be at an adequate level for the wartime environment, it has been suggested by the Army that all data be purged at time of deployment except that which is nonsensitive and/or complies with the Geneva Convention statute.

The concept will decrease the security risks on the battlefield, but may increase system vulnerability at the deployment site(s) during the data purging process. Successful tampering (i.e., wire tapping, counterfeit TID's, etc.) with the TID's at the deployment location could allow the adversary to surreptitiously collect large amounts of very useful strategic information. Therefore, any SDT system design must include very strong security measures during the operation to insure that the data purging operation does not provide any information for the adversary.

There is a temptation to consider a list of requirements, such as that presented above, as a set of absolutes. It is useful in the consideration of a new capability to remember that it generally replaces an existing system, which itself has weaknesses. In the case of the SDT, its use in peacetime generally replaces records often replicated at various levels within the chain of command, and accessible by a variety of individuals. **The information that could be carried in a tag during wartime is currently embodied in some form within existing mobilized forces.**

While it is desirable that a new system such as the SDT increase of the overall level of security, it should be remembered that **a certain amount of risk is already being accepted, and no new system is a cure to all existing problems in any area, including security.** With that caveat in mind, let us examine the inherent security characteristics of the SDT system.

3.2.2 Inherent Security Characteristics of the SDT Concept

At its most basic level the SDT represents a distributed data base in which the data has been distributed to what is probably the maximum

possible extent; the data is carried by the individual soldier. As described below, such a system architecture has both positive and negative security implications.

Before describing the security implications of the SDT system, it is important to note that there is not yet a precedent which establishes the level of security inherent in such portable data carrier systems. Much information has been exchanged regarding the relative "difficulty" associated with viewing and/or altering the data stored in one's own tag, and limited pilot experiments have been performed in areas such as the financial smart card application. However, several issues must be considered in light of these claims:

- All experiments involving secure portable data carriers (predominantly smart cards) are in the pilot stages and, consequently, there is a lowered incentive for the criminal to breach the system. In fact, it would be unwise for the system attacker to make public any successful attack while the system is in the prototype state. His hope would be that the system would, at some point, be made commercial and that his particular attack methodology would reap great rewards.
- The financial smart card systems have never been subject to an independent security audit, and claims are made based on manufacturer's data only. In addition, the underlying hardware/software design of the systems has also been kept secret. This is in direct violation of general security practices, since it must be assumed that any design will ultimately be uncovered by an adversary.
- Computer literacy and access to computing equipment by a significant portion of our population insures that the hardware and knowledge exists to at least attempt to compromise such a system. The cumulative man-hours of unauthorized attempts would be significant, and should any user be successful in his attempt to breach system security, his methodology could spread rapidly to other interested users in the system.

3.2.2.1 Positive Security Implications. In terms of personal information, a portion of the ability to protect information is given up when it is placed in another's safekeeping. Because the SDT retains personal information with the individual, it could be surmised that the SDT information

itself is in the hands of its ultimate protector, and has its analog in one's wallet or purse.

Another inherent security feature of the SDT is the fact that it is somewhat difficult to counterfeit. While a simple metal dog tag or magnetically-encoded card (such as a credit card) can be easily manufactured or altered (sometimes using only common, household items), a significant investment is needed to design and produce working units of the contemplated SDT. The issue of counterfeiting is therefore reduced from a mass population problem.

The SDT system would augment a variety of centralized data base management systems. Without the SDT, these systems operate either in a "star" configuration (with a high volume of data movement between transaction points and the central data base), or in hierarchical configurations in which local copies of the data base are maintained and periodically used to update the central data base. In either the star or hierarchical arrangement, there are:

- Opportunities for data compromise by insiders
- Opportunities for the unauthorized monitoring of data transmissions
- Difficulties with providing a given level of computer security due to the large volume of transactions.

The SDT changes the architecture of the involved information systems to the point where the number of inquiries to a central data base should be reduced, as would the need to maintain so many local copies of the same information. It can be postulated from these results that **the presence of an SDT system could implicitly improve the security of the ADP systems with which it interfaces.** The reduction of traffic could allow a better auditing of the central data base. Periodic (and possibly covert) comparison of tag contents with the data base could provide some protection from unauthorized alteration of data.

3.2.2.2 Negative Security Implications. The distribution of data within the SDT system has its potential vulnerabilities as well as its strengths. While distributing the data to the person most inclined to protect it is a strength, so too does it represent a temptation, as that individual is

also most likely to gain from the fraudulent alteration of some data elements. While there are parallel vulnerabilities in a variety of distributed, paper-based information systems (such as employee timecards), this is an aspect of the system that must be considered.

While the SDT itself would be difficult for an individual to counterfeit, the proliferation of personal computers, SDT tags and terminals, sophisticated hardware and software resources in universities, and the like present resources for overcoming this obstacle. The design of a widespread system such as SDT also results in information, the dissemination of which could proceed rapidly through both authorized and unauthorized channels. This information also represents an important resource to potential system penetrators.

Although there may be an obstacle of equipment associated with the penetration of the system by individuals, that is not necessarily the case with organizations or potential adversaries. Given enough incentive, even the barrier of high initial investment will not deter the most serious criminals. Further, it is likely that some tags, terminals, and information will fall into the wrong hands. **It must, therefore, be assumed that functionally equivalent prototypes of such items as the SDT could be manufactured by unauthorized sources.**

3.2.2.3 Consequences of Inherent Security Implications. The SDT concept presents both strengths and weaknesses in provisions for data security. In large measure, both strengths and weaknesses follow from the lack of central control. Neither authorities nor potential system penetrators have immediate access to the tags and the data contained therein once the tags have been distributed. In some measure, the same situation applies to system design information and a given individual's password (or its analog). **Another security threat is the soldier mistrusting the tag, and therefore discarding it during critical wartime situations.**

This situation has important impacts on the present design effort. Operational security procedures must be superimposed on whatever security attributes the SDT design possesses inherently, or which can be designed in. It is the role of these safeguards to minimize the probability that:

- (1) A successful attack on one element of the system (such as a single terminal or card) can occur.
- (2) Should a successful attack occur, that its effect would have only a minimal propagation throughout the system and would not significantly compromise the overall system.

Before examining potential safeguarding techniques, it is useful to first review potential threats to the SDT system.

3.3 Potential Threats to the SDT System Security

The threats to SDT system security occur in all aspects of the system development and implementation. The SDT system has yet to go through the stages of detailed design, production, fielding, and support. Incentives for security breach exist at all these levels, and their relative magnitude depends on the ultimate risk/reward relationship. Several points in the life cycle and design of the SDT system present particularly significant risks of attack. Characteristics of such points are existing concentrations of data, opportunities for sequential access to many tag's worth of data, or opportunities to compromise the usefulness of the entire system. Another important concern is the disclosure of information which could cause singularly high damage to an individual soldier or installation. The various major points of potential vulnerability and methods of attack have been identified as:

- SDT system design and manufacturing sites
- Hijacking of SDT system components
- Counterfeiting
- Unauthorized tag data alteration
- Alteration of tag interface devices
- Detection of the presence of the tag on the battlefield.

These are discussed below.

3.3.1 SDT System Design and Manufacturing Sites

The primary assumption in any security system is that its original design is free from inadvertent errors and deliberately designed security trap doors. The trap door refers to a mechanism which has been covertly designed into the data tag system which could then be used at a later date to override the security measures, or poison the data base. Examples of trap doors might include:

- Design of the Soldier Data Tag internal circuitry such that input of a specific data stream to the tag causes a series of unauthorized actions to occur. These might include alteration of financial account balances, for example. In wartime, they may allow accessibility of sensitive data within the tag.
- Application software which has hidden features that can be activated through specific sequences, passwords, etc.
- Hardware and software changes in the Soldier Data Tag peripheral equipment which allow for covert monitoring of the data tag information transfer.

In the design review of software it is extremely difficult to analyze the ramifications of the code on a line-by-line basis. Even if this were to be accomplished, it could be possible to hide these trap door features in a manner such that they would be literally impossible to detect.

The hardware designer may also have incentive to include trap door features. Again, detailed examination of a large, complicated digital electronic circuit is difficult to perform and, subsequently, to reverse engineer, in order to document all of the possible functions of the equipment. This security problem has very serious ramifications since, in essence, the system's attacker is building in a successful system at the point of design. It would therefore be likely that such an attack could go unnoticed until its effect on the entire system was catastrophic.

It is difficult to assess how serious this problem will be for the Soldier Data Tag system. However, several points listed below may aid in quantifying the problem:

- The Soldier Data Tag System is not a secret; that is, the fact that the U.S. Government is examining a portable data carrier concept for use by the U.S. military in 1987 has been stated in public conferences, magazines, and newspapers, and in scientific journals.
- The system is in the concept generation stage and no detailed design specification currently exists. It would be far easier to install trap doors in the system as it is being initially designed rather than attempting to place a modification into an existing design of hardware or software. The latter is likely to be more difficult and likely to be detectable.
- If the Department of Defense implies the possibility of a high reliance on a Soldier Data Tag concept for military tactical operations, hostile nations may attempt to infiltrate the research and development phase of this work in order to influence its ultimate design.

3.3.2 Hijacking of SDT System Shipments, or Large-Scale Counterfeit of SDT Systems

The hijacking of a large amount of Soldier Data Tags and/or associated tag interface devices is a possible system attack. The information gained by such an action would be largely related to identifying the overall systems design, and not an extraction of pertinent military data. This is because, at the point of shipment, SDTs are likely to be loaded with only manufacturer's tag information and nothing specific to the soldier. While this is a possible threat, the use of shipment numbers and audit trails such as that employed by the financial industries, would allow the Army to immediately identify when shipments have been stolen.

The infusion of a large amount of counterfeits into the system is also a possible threat. The incentive for such a threat might be to place nonsecure trap door devices into the existing system structure. Again, to guard against this possibility, extensive use of shipment audit trails must be maintained.

3.3.3 Unauthorized Alteration of the Tag Data

This threat refers to the changing of data contained within the SDT by either an individual (the owner of the tag, perhaps) or an organization. From an individual soldier's standpoint, the main incentive for such a system attack is probably for financial gain, or to be granted privileges such as access to certain buildings, etc. From an organization's standpoint there are two distinct incentives. First, since the SDT conceivably identifies the soldier as a valid U.S. Army soldier, an organization could infiltrate the ADP system by posing as an authorized U.S. soldier appropriately manipulating the tag data. The second incentive is to sabotage the SDT system by injecting bogus information.

3.3.4 Counterfeit Tag Threat

The specific incentives for the counterfeit tag manufactured by an organization are described above under system shipments. It is not expected that counterfeiting of tags on an individual basis is a significant threat. The incentive for a soldier to manufacture a counterfeit tag is far overshadowed by the cost of developing such a counterfeit.

3.3.5 Alteration of Tag Interface Devices

From the standpoint of data concentration, it is valid to believe that an organization interested in breaching the security of the SDT system may strike at the tag interface device level, since data tends to concentrate there. An individual's incentive for attack of the tag interface device is low, and probably limited to destruction or sabotage of an individual reader. An organization, on the other hand, could infiltrate the design of the tag interface device in order to perform either information logging or system sabotage. Information logging through some type of wiretapping would allow for things such as strength accounting. In addition, by changing the operation of the tag reader somewhat, sabotage could also occur in both directions. First, the tag interface device could be programmed to destroy, or more appropriately, alter tag data in some matter as to make it useless in the future.

For example, soldiers' critical records could be altered. In addition, bogus data could also be sent to the automated information system points. Protection from this threat is provided by design audits and operational security procedures.

3.3.6 Detection of the Presence of an SDT on the Battlefield

A concern of the wearer of the SDT is that in a wartime situation the tag cannot be used to identify the position of the camouflaged soldier. The project team is aware of the following methods for detecting soldiers in tactical situations:

1. IR Photography
2. Chemical Detection
3. Sound Detection
4. Electronic Detection
5. Visible Light (reflection)
6. Radar Detection.

IR photography, in effect, measures the heat generated by specific items (particularly bodies or equipment). Chemical detection is made by identifying the odors associated with specific ethnic groups. Electronic detection is accomplished by picking up electronic signals or frequencies emitted by the equipment used by the soldier, i.e., computers, communication equipment, generators, and motors. The sound detection is mainly to identify the sounds of metal touching and of movement.

The SDT as currently produced is unlikely to produce a signature which can be identified by the enemy. In Battelle's opinion the soldier's body and equipment would be the major source of detection and not the SDT.

3.4 Potential SDT System Penetration Countermeasures

The SDT concept brings its own set of potential countermeasures which can be designed into the system. Before concluding this discussion of

SDT security, it is useful to review these opportunities and their potential impacts.

3.4.1 SDT Onboard Security

3.4.1.1 Onboard Processor. If the tag contains some type of electronic memory, then an on-board microprocessor can be used to restrict access to portions of the memory. There has been precedent set for this type of technology in the current generation of smart credit cards. Basically, the microprocessor serves as a traffic cop, and routes information into and out of memory. Typically, the authorization is provided by supplying some type of authentication number, and this is compared within the microprocessor's memory. Segmentation of the memory can be performed to allow information to be accessible to the outside world without the microprocessor's intervention and to allow other pieces of information to be protected with varying levels of security under microprocessor control. This would then allow for different organizations to access different portions of the memory. The advantage of onboard processing is that proper authentication codes and information cannot be extracted from the memory. The on-board processor can also perform a semi-permanent "lock-out" if the proper codes are not entered. With the use of optical storage techniques, information is always accessible, although it may be encrypted. The key management problem may be such that the encrypted information can be decoded.

The potential disadvantage with the personal identification number is that the soldier or other authorized party is required to memorize an access number. Studies in the commercial sector have shown that individuals are apt to carry their personal identification numbers (PIN) with their credit card because they cannot remember the password. In wartime situations, such a system could be hampered because the soldier may be stressed to a point where he may forget his number. Also, medical information would need to be unprotected since an unconscious soldier would not be able to provide his PIN so that medics could read his emergency medical data.

The current prototype design uses a microprocessor chip and a separate memory chip, interconnected via a set of wired connections. By removing the encasement and probing these interconnections, it could be

possible to bypass the microprocessor control and directly examine the contents of the SDT's memory. In the final SDT design, it is probably most desirable to implement the embedded electronics as a single, customized circuit, rather than multiple interconnected chips. In this way, data and processor instructions do not appear on any input/output pins, and the software program and associated data are externally invisible.

3.4.1.2 Special Purpose Hardware. In addition to onboard microprocessors, there are other hardware methods of providing levels of security on the SDT. For example, the Intel 27916 KEYPROM memory is a two-chip set that provides a hardware authorization procedure. Geared primarily toward terminal authorization, the KEYPROM device is flexible and can be configured to meet the needs of many user-security systems. The price for the chip set is \$45 in 10,000 quantity and a KEYPROM chip could be required in each SDT. Other electronics manufacturers are also beginning to introduce similar products as the need for security systems continues to rise. None of these products currently address the specific needs of the SDT, but their emergence into the commercial marketplace will bring cost effective security hardware techniques within reach of the SDT system.

3.4.2 Authentication Technologies

An alternative to personal identification numbers was discussed in an earlier section and presented systems which can analyze biometric traits. The data storage requirements for such systems is relatively low and certainly within the realm of most technologies being considered for the SDT. It would be advisable for the highly secure applications of the data tag to incorporate some type of biometric feature analysis in conjunction with other security measures.

3.4.3 Combination Electronic Memory and Optical Memory

One of the security problems identified is the possibility of the soldier discarding his own tag because of the lack of confidence in its

security. A possible data tag configuration mentioned earlier was the combination of the high capacity storage stripe with the changeable electronically erasable memory. A system which combines the two would have several security advantages. The relative functions of the two technologies would be:

- Electronically erasable memory (with perhaps a microprocessor)
 - This memory would be responsible for storing a small degree of highly sensitive data.
- Optical stripe
 - This storage device would be responsible for the archival storage of data which would be useful to ADP Systems, etc., but is nonsensitive.

In a battlefield situation it is likely that the archival data could provide tactical advantages to the Army. Knowledge of a soldier's background training, for example, would be valuable information. If these data were to fall into the hands of the enemy, many inferences could be drawn regarding purpose of missions, company strength, etc. Current SDT system plans for a battlefield tag call for only Geneva Convention data to be stored. Therefore, a potential tag structure which combines the two technologies might allow for the optical storage stripe to be physically removed when a soldier is deployed, removing all sensitive data.

While encryption technology provides a high level of data security, the most vulnerable point in the system is the security of its keys. An encryption system capable of a high level of security for a device used as broadly as that proposed for the soldier data tag would probably present a key management problem of staggering proportions; however, on a much smaller scale it would be feasible and is probably practical. If the soldier data tag memory space is considered to be a scratch pad, it would be possible to use a device to carry secret orders from one destination to another using an encryption algorithm and key only known to those two sources. Once the message was delivered, it could be erased if an EEPROM is used, or obliterated if an optical stripe is employed.

3.4.4 Data Encryption with the SDT

Since the result of encrypting a stream of digital data is another stream of digital data, the SDT system is fully compatible with most data encryption schemes. A fundamental issue in applying data encryption to the SDT system is the matter of key management. In small, tightly controlled systems, the data encryption keys may be known only to several users. In such systems, high levels of security can be maintained by the integrity of its users. In the case of the SDT system, with millions of tags in distribution along with thousands of sites capable of reading these tags, the key management problem becomes significant. A public key algorithm seems to have the attributes necessary for such a widely distributed system: low requirement for key replacement to maintain security, and flexibility in application of encryption processes.

Relationships between threats and countermeasures are depicted in Table 3.2. The first column is the threat category; i.e., the general mechanism by which the threat operates. In all threats the objectives can be assumed to include access to information and addition of new (erroneous) information. The second column, labelled "Perpetrators", identifies the primary beneficiary of the attack. "Target" refers to the component of the SDT system most directly involved in the threat. Column number four is a subjective estimate of the degree of difficulty and resources requirements of the attack. An example of a "High" resource requirement is tag counterfeiting, which requires integrated-circuit manufacturing facilities. The fifth column is a subjective estimate of the likelihood of occurrence. Column six identifies an existing system which is susceptible to the same threat, if one can be identified. The next six columns indicate whether the corresponding countermeasure is at all effective against the threat. Countermeasures are given in general categories described by their operation. Implementation of these measures is a separate issue.

- **Design audit** - careful control and review of the design process as well as the component designs. This is to prevent any small group of people having independent control of the design.

TABLE 3.2. SUMMARY OF SECURITY THREATS AND COUNTERMEASURES

Threat	Perpetrator	Target	Resources	Prob	Precedent	Countermeasure
Trapdoor	Mfr	Tag, TID	Mod	Mod	ADP Sys	Design audit
Hijack	Enemy	Tag, TID	Low	Mod		Tag serialization
Hijack	Criminal	Tag, TID	Low	Mod		Operational security
Counterfeit	Enemy	Tag, TID	High	Mod	ID	Tag serialization
Counterfeit	Criminal	Tag	High	Low	ID	Verification
Counterfeit	Mfr	Tag	Low	Mod		Audit trail
Wiretapping	Enemy	TID	Mod	High	ADP Sys	Encryption
Masquerade	Enemy	Tag	Low	High	ID	Verification
Masquerade	Criminal	Tag	Low	Low	ID	Verification
Masquerade	Soldier	Tag	Low	Low	ID	Audit trail

- **Encryption** - storage of all information in a form not useful without knowledge of a decryption key.
- **Authentication** - any of a number of methods relying on what a soldier knows (password, Personal Identification Number) or his fingerprints, voiceprints, to control access to the system.
- **Audit trail** - complete records, maintained by the host ADP system, of all transactions involving each card in the system.
- **Verification** - comparison, during a routine transaction, of data in a tag with reference information from the master data base.
- **Operational security** - procedures employed by users and controllers of a system to augment the security provided by the basic system.

3.5 Conclusions

It is useful at this stage of the SDT's life cycle to examine potential countermeasures to the data security threat. On the other hand, the intermediate state of the SDT system design makes it impossible at this time to recommend categorically the specific use of some of the various security tools that have been described in this chapter, or to absolutely evaluate the level of security obtainable in the ultimate system. As indicated, a variety of techniques are available, both technical and operational, which can be applied to protect against given threats. Before stating our conclusions with respect to the overall issue of SDT system security, it is useful to note some specific recommendations.

It is crucial that the threat to the SDT system be continually reevaluated:

- As the design of the SDT system evolves
- Whenever a new application is proposed for the fielded system
- Whenever there is a change in the technology or configuration in the fielded system
- As new technological tools become available to potential system penetrators.

While there are technological countermeasures, it is apparent that operational countermeasures will also need to be employed. Examples of where operational safeguards will probably have to be employed include:

- In the design process, to insure that a combination of compartmentalization and independent review prevents the inclusion of "trap doors" which could be utilized for future penetrations
- In the distribution process, where tracking techniques will be needed to insure that counterfeit tags are not injected into the pipeline
- In the control and utilization of terminals in the deployment process, to insure that terminal sabotage does not cause critical delays or confusion

- In the system support phase, where configuration control techniques will be needed to insure that new applications do not accidentally or intentionally damage or penetrate the system
- In the auditing process, where covert checks can be made to insure that the contents of individual tags still match the approved data maintained centrally.

As indicated above, while not possible to be categorical with respect to the set of technological countermeasures which should be employed within the SDT system, there are nevertheless some likely choices to highlight:

- It is unlikely that security in such a widely distributed and publicized system can be maintained through the use of "secret" passwords, encryption algorithms, or integrated circuit design. Instead, near-term solutions will most likely involve:
 - The use of public key method of data encryption
 - The use of a robust hardware architecture with some capability for electronic destruction of critical data paths.
- It is unlikely that any absolutely foolproof techniques will be found to guarantee the protection of militarily-critical information in the tag. This means that:
 - Operational approaches will be needed to protect information on the tag needed on the battlefield and of military importance to the enemy
 - Attention will have to be paid to human factors so that the soldier will in general not want to discard the tag in combat.

It should be noted that **the inability to guarantee the security of classified information is not a special weakness of the SDT**; the same is true of information that is carried into battle in the heads or pockets of soldiers. Paper copies of orders, pictures of family members, and other material commonly carried into battle by soldiers represent a body of potentially significant security leaks. All that can be done in the SDT design is to make information difficult (though not impossible) to obtain, and to parcel the information out so that the loss of one part of it does not compromise the whole.

In conclusion, while it will not be possible to guarantee the security of data contained in the SDT system, or the integrity of the system itself, a combination of the technological opportunities presented by the tag, the array of operational safeguards which could be employed, careful consideration of data and applications to be implemented using the tag, and care in the partitioning of militarily significant data will likely provide an adequately secure and militarily useful system.

3.6 Recommendations Resulting From The Security Considerations Section

Based on an analysis of the SDT concept and its underlying security requirements, Battelle provides the following recommendations:

- The tag design should provide secure segments of memory in the tag, even if none of the initial applications use it. Future evolutions of the system for peacetime and wartime are likely to require such protection.
- A detailed study of the information handling and processing needs on the battlefield should be performed. Although the current SDT concept specifies a tag which contains only Geneva Convention data during wartime, it is possible that some levels of sensitive data could be stored on the tag. This information could be protected via encryption schemes, on-board protection, and even physical protection of the tag itself. The study may reveal that various levels of data sensitivity exist. These could be compared against the security capabilities of the SDT, and potential applications for more sensitive command and control information could be identified.
- Develop operational security procedures for SDT system design and fielding. This includes design audits for the tags, TID, and applications software.
- An independent security audit and review should be performed on the SDT hardware/software. Such a review would reveal design flaws in the security system, and could reveal useful information from the prototype system.

4.0 COMPONENT LEVEL DESIGN ISSUES

The objective of this section of the report is to describe the design issues specifically related to the physical design of the system. For the purposes of this section, the "system" is defined as the soldier data tag, tag interface device, and embedded software. Described herein are the design issues surrounding the design and fabrication of the data tag. It is broken down into five areas:

- **4.1 Information Storage Technology for the Tag.** Includes a discussion of the relevant technologies and their trade-offs in design.
- **4.2 Materials Technology for the Tag.** Describes the materials issues surrounding the fabrication and survivability of the tag. A glossary of terms is included at the end of this section.
- **4.3 Tag Interface Device Design Issues.** Includes a discussion of tag interface, host interface, software, and communication technologies. Also addresses issues associated with metallic contact and noncontact interfaces.
- **4.4 Conclusions.**
- **4.5 Recommendations for Component Level Design Issues.**

4.1 Information Storage Technology for the Tag

The Soldier Data Tag has the main function of portable transport of data. The Army had identified in the original RFP that Battelle's investigation be limited only to microelectronic data storage technologies. The rationale for this limitation was that the original experiments with the Soldier Data Tag had taken place using that technology and no other medium was readily available to demonstrate and test the concept (i.e., optical reflective stripe cards, high capacity magnetic stripe cards). However, there are technologies other than microelectronic memory which are capable of the non-volatile storage of information, and therefore it is useful to examine the spectrum of technologies. In this way, the design of the SDT can be application driven rather than technology driven.

Before continuing with a discussion of data storage technologies, it is useful to first discuss the general concept of digital information storage. A double-sided typewritten page will require approximately 2,000 bytes of storage. Using this as a guideline, the following list provides the information storage capacities of some common media:

- A 8k-byte memory chip can store 8 pages of text. (The current prototype SDT.)
- A 360 k-byte floppy disk can store 180 pages.
- A 10 mega-byte hard disk can store 5,000 pages.
- A 5.25" laser disk can store 200,000 pages.
- A 12" laser disk can store 500,000 pages.

There are several criteria which must be met by any SDT device, including:

- **Nonvolatile data storage.** Power is not required to retain data.
- **Data is field-updateable.** This implies that there is a method of changing the data contents of the tag in the field. Note that erasability is not a strict criterion. A storage technology which offers large amounts of storage could function as well as an erasable technology with a more limited storage capacity.
- **Contains sufficient storage capacity for the application.** A specific amount of data cannot be defined as yet because a system specification has not been established. The current experiments utilize a 64K-bit tag. However, it may be feasible in certain tactical applications to use a tag with much more limited data capacity.
- **Information on the tag is machine readable.** This implies the use of digital storage schemes.
- **Portability.** The data storage method must be capable of being stored in a portable, carryable package which is no smaller than the current dog tag, and no larger than the identification card.
- **Survivability.** The package must maintain data integrity under the battlefield environment, including some

level of NBC contamination yet to be established by the Army.

- **Security.** The technology must be capable of enforcing some degree of system and data security.

Based on the above requirements, several storage technologies can be identified. These include:

- EPROM - UV erasable, read-only memory
- EEPROM - electronically erasable read-only memory
- Magnetic stripe
- Optical stripe.

EPROM's have been used widely in smart card applications because they are relatively inexpensive and offer a chip geometry which is 80 percent smaller than an EEPROM of comparable storage capacity. The disadvantage of EPROM's in the SDT application is that they cannot be selectively erased. The magnetic stripe is also feasible based upon the updateability constraint, but data integrity would likely suffer because it is not survivable in the rugged environment.

With the above in mind, two technologies remain. They can be further evaluated based on their relative individual merits and their impact on the necessary reading technology.

4.1.1 Comparison of Technologies

There are two approaches to providing a long useful life to an individual tag: it either has to use a conventionally erasable memory or have an extremely high storage capacity. The only technology which provides erasability is the EEPROM. Although this is one of the more recent developments in digital electronic memory technology, it is already well down the favorable price capacity curves characteristic of that technology. (See Table 4.1.)

As seen in the table, electronic technologies have cost reductions as the technology matures and sales volumes increase. A dramatic example of this is found in the 256 K-bit dynamic RAM (random access memory). In January of 1984, the integrated circuit was available for \$92. January, 1985, the

TABLE 4.1. REPRESENTATIVE MEMORY PRICE DATA

Item	Introductory Price	Today's Price	Projected Price (1987-89)
2K x 8 bit	\$27 (1982)	\$10	\$ 2
8K x 8 bit	\$95 (1983 1/2)	\$25	\$10

cost of this chip had dropped to \$12 as they began to see significant usage in office automation systems. Today, the cost has continued to decline and they are now available for \$3.40!

EEPROM's are currently available with 64 K-bits of memory, in contrast with EPROM's which are approaching 512 K-bits. In the next few years, it is expected that the EEPROM will be available with 256 K-bit capacity.

Optical memory media, as represented by the laser stripe cards, can provide the capacity for an extremely high amount of data. While optical data disks are commercially available, there have been unexpected delays in commercialization of the card concept. **The reader manufacturers have been unable to publicly demonstrate a working system as of May, 1985.** An intriguing possibility is the combination of electronic and optical memories in the same card. The electronic memory can provide a reuseable "scratch pad" area while the optical memories can provide archival memory capabilities.

Another intriguing possibility is the inclusion of a microprocessor in the tag itself. The technologies used are, by definition, limited to either electronic memory or a combination of electronic and optical, where the optical would not be accessible to the onboard processor. Potential advantages of including a processor on the tag itself accrue in the areas of security and, at the system level, in simplification of tag interface device design. In general, 8-bit microprocessors suitable for this function are available for \$1-5. It should be noted that while the microprocessor-based SDT prototype is a Datakey product, other companies currently offer a EEPROM-based data carrier. Quartic Systems, Salt Lake City, use a 2K-byte module for data transfer.

The physical characteristics and the cost of a tag based on electronic memory would be controlled by the connector design as much as by the memory itself. Problems with metallic contacts are discussed in the Tag Interface Device section, along with several alternative connection technologies. The relatively limited storage capacity of current EEPROMs make the control of data formats and organization very important. This issue is also discussed in more detail earlier in this report.

4.2 Materials Technology for the Tag

The objective of this task involves identifying alternative polymeric materials for the SDT, examining requirements and trade-offs, and analyzing the impact of material selection on manufacturing costs. It is expected that this evaluation process will provide several options for the selection of the protective plastic encapsulating material(s) and their associated costs and benefits. The subsection is organized into the following areas:

- **Information Analysis.** Includes methods used for identifying the types and properties of candidate polymeric materials.
- **Identification of Preliminary Performance Requirements.** A documentation of physical, mechanical, and electrical properties; survivability of the SDT including chemical, nuclear, electromagnetic, and microwave radiation resistance; and surface information analysis.
- **Summary of Candidate Polymers.** A listing of advantages and disadvantages of the candidate materials along with reasons for elimination.
- **Conclusions.** Final evaluations of the chosen materials and additional study results.

4.2.1 Information Analysis

4.2.1.1 Why Plastics? In examining candidate materials for the SDT it was necessary to briefly assess the advantages and disadvantages of metals and ceramics as compared to polymeric materials. In general, ceramic

materials are brittle, easily fractured, and require high processing temperatures. If the material was porous it would be difficult to decontaminate and would have to be discarded upon exposure to toxic agents. Ceramic materials are also usually quite expensive.

Metals have traditionally been used as the material for the military identification tag and have proven to be sufficient for its present use. However, metal is not very well suited for the basic encasement material of the SDT. (As a shielding material for microwave and electromagnetic interference (EMI), metals may be the most suitable material. Several shielding concepts are described later in this section.)

Rather than extremes of a single property, the following combination of properties was considered in choosing a polymeric material over a metal or ceramic as the SDT encasement.

1. Plastics can be fabricated in liquid form; therefore, the material is easily processed.
2. Parts can be made in one operation without generation of large amounts of scrap.
3. Since coloring is not restricted to the surface, damage due to abrasion or scratching is less obvious than in the case of a coated metal.
4. Plastics are corrosion resistant, unlike many metals.
5. Plastics are available in a wide range of solvent and chemical resistances, as well as varying degrees of strength, flexibility, and toughness. Many fiber reinforced plastics have high strength/unit weight ratios close to those of many metals.

The information gathering and analysis included a trip to Datakey Corporation to analyze nonproprietary data tag information and a computer search of several data bases to identify potential polymer candidates.

Site Visit. Datakey, Inc. in Burnsville, Minnesota provided the tags used in the Army's concept demonstrations. Characteristics of this tag can provide a starting point for identifying materials issues. Production steps involved in the manufacture of the data tag were carefully examined. The memory chip is assembled by an outside manufacturer. Datakey picks up the

production process with the application of an unfilled epoxy encapsulant to the microchip as a protective cover. The data tag is produced from an insert injection molding operation using polyphenylene sulfide at 1000 lbs pressure, 600°F, and a 15 second dwell time. After each major production step of the tag, a quality control test is performed. A total of nine quality assurance tests are performed throughout the SDT production. The final test performed on the finished data tag involves a thermal cycling test carried out between 0-70°C for 12 cycles per 24 hours. Datakey presently owns a microprocessor controlled injection molder which can be fitted with multiple cavities on a carousel and is capable of producing up to 6 data tags in a single cycle. However, the large number of hand operations involved in the current prototype data tag fabrication is not appropriate for large volume production. To meet the production volume of tags required for the SDT system, an automated facility will be necessary.

Midway through Battelle's study, Celanese Corporation, a supplier of Liquid Crystal Polymer (LCP), traveled to Datakey in order to determine the applicability of their LCP to a high capacity tag application. Results from this visit provided Battelle and Datakey an opportunity to evaluate an alternative polymer in the tag production. Both Datakey and Celanese reported good results from the pilot run. This run gave Battelle the confidence that the present fabrication process will be able to handle a new material if the Army should decide to proceed with another polymer.

Results of Computer Search. Battelle accessed two commercially available computer data bases listing plastic materials and properties: Polyprobe and Plaspec. Polyprobe is an on-line, computerized data base system which allows information to be obtained on most currently manufactured plastics. It provides over two dozen properties for over 8100 commercially available plastics. The Plaspec data base provides processing information and various properties for over 40 families of materials. Because mechanical data are usually more updated in these data base systems, preliminary mechanical property data were searched in these systems including a range of property values for tensile strength (9,000-11,000 psi), tensile modulus ($.5-1.5 \times 10^6$ psi), and elongation (0-2 percent).

Contact with Commercial Suppliers. Along with the other methods of acquiring data, Battelle project members contacted commercial suppliers of base resins as well as resin compounders. Company names and phone numbers can be found in the appendix.

From the information acquired through the computer search, the supplier contacts, and recommendation from the project team, a list of possible candidates was prepared. Table 4.2 lists the polymers evaluated and highlights their characteristics. In this table, a number of relative terms are used; "inexpensive" usually means \$3-\$4 per pound, "moderate" is \$5-\$10, and anything over \$10 is "expensive".

Included in this list are two thermosets, diallylphthalates and phenolics, and the remainder are thermoplastics. Each of these materials will be discussed in greater detail below.

4.2.2 Identification of Preliminary Performance Requirements

As we began to examine the performance requirements for the SDT, it became apparent that the mechanical properties of the encapsulating material, although important, were less critical than the physical, electrical, and chemical properties. Mold shrinkage, volume resistivity, moisture absorption, flammability, and chemical resistance are considered to be the most critical properties to be optimized for producing the all around best SDT. **Low part shrinkage is a critical requirement**, since part shrinkage has been found to damage the microchip. Moisture absorption can affect the volume resistivity which can affect static discharge. It is necessary that the volume resistivity remain between 10^7 to 5×10^9 ohm-cm, since major fluctuations outside this range can result in electrical mishap. A flammability rating of UL94, V-0 and stringent chemical resistant requirements were imposed on the SDT as two important survivability parameters.

Additional properties examined were heat deflection temperature (HDT) at 264 psi, and the ability of the polymer to be nonskin sensitizing. Table 4.3 indicates our recommendations of parameters for several mechanical and physical properties for the SDT. It should be understood that the values shown are based solely on our experience in dealing with polymeric materials.

TABLE 4.2. CHARACTERISTICS OF CANDIDATE POLYMER CLASSES

Polymer	Characteristics(1)
Diallylphthalates	Thermoset, excellent dimensional stability, chemical resistance, mechanical strength, and heat resistance. Can attain UL94, V-0 with additives. Inexpensive.
Fluoropolymers	Thermoplastic, high service temperature, perform well in chemical environments, do not support combustion or promote flame spread. Highly corrosive to molds/processing equipment. Expensive (as high as \$35/lb in some instances).
Liquid Crystal Polymers	Thermoplastic, relatively new product, good HDT's; chemical, UV, and flame resistant, Easily moldable. Moderate to expensive(2).
Nylons	Thermoplastic, tough, high strength, good wear and abrasion resistance, good chemical resistance, FDA approved. Must use Nylon 12 or other low moisture absorption resins. Moderate price.
Polyetheretherketone (PEEK)	Thermoplastic, excellent thermal stability, UL94, V-0, resistant to a wide range of solvents, tough, strong, rigid and good load bearing properties. Expensive. (\$35/lb)
Phenolics	Thermoset, good heat and chemical resistance, excellent dimensional stability, easy moldability. Low cost.
Polyacetals	Thermoplastic, unique balance of mechanical, thermal, chemical and electrical properties. Excellent moldability. No UL94, V-0 rating.
Polyamide-imide	Thermoplastic, good dimensional stability, impact resistance, superior mechanical properties from -40 to 400°F, UV stable. Expensive.
Polyarylsulfone	Thermoplastic, long term thermal stability, good ductility retained from -100 to 200°C. Combustion resistance without additives. Expensive.

(1) Included are highlights for each material.

(2) Celanese has agreed to make LCP cost competitive with PPS.

TABLE 4.2. (Continued)

Polymer	Characteristics(1)
PBT/PET	Thermoplastic, excellent moldability, broad chemical resistance, high heat resistance, good lubricity and wear, UL94, V-0 with additives, FDA approved. Inexpensive.
Polyetherimides	Thermoplastic, high heat resistance, broad chemical resistance, stable over wide temperatures and frequencies. Moderate cost.
Polyethersulfones	Thermoplastic, thermally stable, UL94, V-0, continuous service temperature 350-400°F. Excellent impact resistance. Moderate cost.
Polyphenylenesulfides	Thermoplastic, material used in present SDT, thermally stable, not affected by moisture, excellent chemical resistance, corrodes processing equipment. Does not support prolonged combustion. Moderate to expensive costs.
Polysulfones	Thermoplastic, good thermal stability and rigidity at high temperatures, good impact strength, continuous service temperature (up to 300°F). Inexpensive to moderate costs.

(1) Included are highlights for each material.

TABLE 4.3. MECHANICAL PROPERTIES FOR RYTON SDT ENCAPSULANT

Impact Strength, IZOD, notched 1/4"	0.9	D-256
unnotched 1/4"	3.0	
Tensile Strength, psi	11,000	D-638
Tensile Elongation, %	0.6	D-638
Tensile Modulus, psi x 10 ⁶	1.8	D-638
Flexural Strength, psi	15,000	D-790
Flexural Modulus, psi x 10 ⁶	1.5	D-790
Deflection Temperature, F @ 264 psi	500	D-648
@ 66 psi	500 +	

Laboratory evaluation of the SDT properties should be made to confirm the validity of the values.

The mechanical properties tend to be the most flexible parameters necessary for the SDT. Properties associated with the Ryton product are probably more stringent than required. Therefore, the mechanical values shown in Table 4.3 may possibly be relaxed.

The values for volume resistivity and mold shrinkage probably should not be relaxed. The operation of the SDT may ultimately depend on these parameters. In the future, it may be necessary to test the effect of moisture absorption on the operation of the data tag.

The most nebulous values appear for continuous service and storage temperature and for heat distortion at 264 and 66 psi. It is the project team's opinion the polymeric encasement will remain intact and will have greater service life expectancy than the microchip.

Datakey Corporation has never tested the operation of the chip outside the temperature limits of -65 to 100°F. However, it is their opinion that the read capability would not be affected by wider temperature excursions, but the millisecond write capability may possibly be lengthened. Datakey is expected to be testing operation from a cold start in the near future.

The final parameter to be considered is the coefficient of thermal expansion. Since the prototype SDT contacts consist of gold plated nickel, the coefficient of thermal expansion of the polymeric material should be similar to the nickel to prevent any delamination or pulling away of the encasement. Nickel is known to have a thermal expansion of 12.8×10^6 in/in at 20°C (68°F). Therefore, similar polymeric materials should be sought.

4.2.3 Materials Research Results

4.2.3.1 Material Selection. Each polymeric class was evaluated with regard to processing constraints, property considerations, and survivability. Each of these factors is discussed in greater detail below.

Processing Constraints. Insert injection molding was the only processing method considered, since volume and speed will have major influence

on the cost/benefit of the encasement. Injection molding techniques can be used for processing both thermoplastic and thermoset materials. The only real difference in these two classes is that scrap thermoplastic can be reground and reused. However, once a thermoset has reacted it cannot be reprocessed.

Table 4.4 summarizes processing data along with other chemical and physical properties of several candidate materials. The Datakey injection molder is not suited for producing large volumes of tags without some manual manipulation, which in turn slows the production rate. However, robotic systems are available which can easily handle a faster production rate and larger volumes.

Each polymeric class has its own processing idiosyncrasies. For example, the diallylphthalates and phenolics are thermosets and must be processed as such. The acetals must be processed between 370 and 400°F and do not have to be dried before processing. The acetal resin sets up fast with little flash and can also be machined like soft brass.

The fluoropolymers usually have high processing temperatures. Because of their chemical makeup, they are corrosive to molds and processing equipment. Liquid Crystal Polymers (LCP) are a newcomer to the polymeric field. These materials have lower molding temperatures than polyphenylene sulfide and are easily processed.

Nylons (polyamides) have a broad processing range, easy processability, and a variety of melt viscosities which allow them to be processed by almost all the thermoplastic processing methods. Nylons must be processed, however, with less than 0.2 percent moisture content to prevent hydrolytic degradation of the melt. Therefore, if bags are left open before processing, drying becomes necessary.

Polyamide-imides, polyetherimides, polybutylene terephthalates (PBT), and polyethylene terephthalates (PET) all absorb atmospheric moisture; therefore, they must be dried before processing.

However, the polyamide-imides and the polyetherimides process at fairly high melt temperatures, while the PBTs and the PETs can be processed between 405 and 500°F. The polyethersulfones and the polysulfones both require high melt temperatures and also require drying before processing.

Polyphenylene sulfide (PPS), the material from which the Datakey data tag is produced, also requires high melt and mold temperatures. PPS is

TABLE 4.4. PROPERTIES AND PROJECTED COSTS FOR SEVERAL INJECTION MOLDING SYSTEMS

PROPERTIES	POLYMER CLASS						
	1	2	3	4	5	6	7
Designation	Polyphenylene Sulfide	Polyphenylene Sulfide	Polysulfone	Polyether Sulfone	PEEK	Polyetherimide	LCP
	RTP-1399 x 50479	J1300/CF/20	J1500/CF/20	J1100/CF/30	J1105/CF/30	J1106/CF/30	LX 178
Processing							
Melt Temp, F	550-650	550-650	600-780	600-780	660-715	640-800	500
Mold Temp, F	180-400	100-400	200-350	200-350	300	150-350	200
Filler Type/Concentration	Glass/30% Conductive Carbon Black	Chopped Pan/ 20%	Chopped Pan/ 20%	Chopped Pan/ 30%	Chopped Pan/ 30%	Chopped Pan/ 30%	Chopped Pan/ 12%; Conductive Carbon Black
Mechanical							
Tensile Strength, psi x 10 ³	11.0	20.0	20.0	30.0	32.0	30.0	23.8
Flexural Modulus, psi x 10 ⁶	1.5	2.2	2.0	2.5	2.5	2.5	2.1
Elongation, %	0.6	2.0	2.4	1.7	1.4	1.4	3.7
Radiation Resistance							
Rods, Gamma Neutron (No property change)	3 x 10 ⁸ 4 x 10 ⁸	3 x 10 ⁸ 4 x 10 ⁸	UK UK	3 x 10 ⁷ UK	1.1 x 10 ⁹ UK	UK UK	5 x 10 ⁸ UK
Electrical							
Volume Resistivity, OHM-cm	10 ⁷⁻⁵ x 10 ⁹	10 ³	10 ⁴	10 ⁴	10 ⁴	10 ⁴	-
Physical							
Mold Shrinkage, in/in-1/8" section	0.0015	0.08	0.05	0.05	0.05	0.05	0.001-.002
Flammability, UL94	V-0	V-0	V-0	V-0	V-0	V-0	V-0
Moisture Absorption, %, 24 hrs	0.02	0.03	0.2	-	0.06	-	-
Heat Distortion Temp, F, @ 264 psi @ 66 psi	500 >500	480 520	370 375	428 -	610 615	410 415	430 -
Chemical Resistance							
Weak Acids	Excellent	Excellent	Good	Good	Excellent	Good	Excellent
Strong Acids	Good	Good	Good	Good	Excellent	Good	Excellent
Weak Alkalies	Excellent	Excellent	Good	Good	Excellent	Poor	Excellent
Strong Alkalies	Excellent	Excellent	Good	Fair	Excellent	Poor	UK
Organic Solvents	Excellent	Excellent	Fair	Poor	Excellent	Poor	UK
Chlorinated Solvents	Good	Good	Poor	Poor	Excellent	Poor	UK
Cost/Pound/1000 lbs	6.50-7.00	10.25	10.25	12.75	35.00	12.75	7.50-8.50

Source of Materials: 1 RTP Co., Minona, Minnesota
 2-6 Wilson-Fiberfil, Evansville, Indiana
 7 Celanese Corp., Summit, New Jersey

also known to cause rapid wear on the processing equipment. The mold is expected to have half of the service life that would be expected for other noncorrosive thermoplastics.

Mechanical Properties. Although the SDT (Soldier Data Tag) is not a rigorous structural application, several properties are considered vital to prolonged and satisfactory service life. These include flexural modulus to minimize bending and consequent stress of the memory chips and circuitry. Similarly, the protective encapsulating system should have a low elongation under stress. Although fracture is generally undesirable, this could alert the wearer/user to potential internal damage. (No specific laboratory tests were performed, but a comparison of the prototype SDT to the current ID tag can be approximated. Based on manufacturers data and tag dimensions, the metal ID tag is over 1.5 times stronger than the SDT in the flex modulus. However, the SDT is slightly stronger in the tensile strength mode.)

Based on the probability for rigorous environmental exposure, the protective encapsulating system should be tough and abrasion resistant. It is not known whether requisite mechanical properties have been rigorously defined by either materials research or micromechanics studies. It is known, however, that satisfactory performance has been demonstrated by a Ryton-based system in a similar application. Accordingly, mechanical properties reported for the Ryton system provide a convenient basis for desirable property specifications unless studies are conducted to demonstrate that other values are either satisfactory or more suitable. Presently specified mechanical properties for the SDT encapsulating system are shown in Table 4.5.

Electrical Properties. Electrical characteristics of the encasement material have a very critical role in the survivability of the SDT. Most integrated circuit chips (in die form) are able to withstand an electrostatic discharge (ESD) of approximately 2000-3000 volts. This should be contrasted with the fact that a build-up of 20,000 volts is typical when walking across a carpeted room on a dry day. One method of protecting the circuit is to place some type of static suppression circuitry on the IC itself. This method is often times too expensive and a more cost effective approach uses limited conductivity in the encasement to provide protection against static discharge.

TABLE 4.5. MECHANICAL AND PHYSICAL PROPERTIES REQUIRED FOR SDT

<u>Mechanical Properties</u>	
Tensile Strength	9,000-11,000 psi
Flexural Modulus	0.5-1.5 x 10 ⁶ psi
Elongation	0.6-2.0%
<u>Electrical Properties</u>	
Electrostatic Discharge Protection Volume Resistivity	10 ⁷ - 5 x 10 ⁹ ohm-cm
<u>Physical Properties</u>	
Mold Shrinkage	<.0015 in/in, 1.8 inch section <.0025 in/in, 1.4 inch section
Flammability Resistance UL94 Specification	V-0
Moisture Absorption	<.02%, 25 hours at 23 C
Continuous Service Temperature	-20 to 140 F
Storage Temperature	-40 to 140 F
Chemical Resistance	Various solvents/chemical and biological warfare agents
HDT, F, @ 264 psi @ 66 psi	To be determined To be determined
Coefficient of Thermal Expansion in/in, F x 10 ⁵	To be determined

However, the conductivity cannot be excessive or electrical shorts can develop between chip contacts. It has been found that an acceptable electrical performance is achieved with a volume resistivity between 10⁷ and 10⁹ ohm-centimeters. This provides protection against static discharge without shorting between contacts. Volume and surface (ASTM D-257) resistivity should not decrease below 5 x 10⁷ either initially or after exposure to conductive

environments. Using a combination of the above approaches, the manufacturer of the prototype tag claims a resistance to static discharges up to 25 KVolts.

Achieving appropriate resistivity in the range specified requires the addition of a conductive material to a normally insulating polymer. Current technology utilizes several types of conductive fillers to produce electrostatic discharge (ESD) protection and electromagnetic (EMI) shielding systems. Such systems are compounded to have resistivities generally ranging from 10^4 to 10^2 ohm-cm. These are achieved by adding such materials as conductive carbon black, carbon/graphite fibers, metal fibers/flakes, and metal coated glass/graphite fibers. Filler choice and amount is critical in achieving the desired level of conductivity. Further, compounding and fabrication factors can markedly influence the level of conductivity.

The accompanying Figure 4.1 shows the critical nature of adjusting conductive filler levels to achieve a semiconductive (10^7 - 10^9 ohm-cm resistance) system. The extremely rapid transition from an insulator to a conductor occurs with a nominal conductive filler change of about 3 volume percent. Although this transition curve is for aluminum fiber, the shape of the curve is generally characteristic for all conductive fillers. Thus, the amount of a given conductive filler must be precisely determined and controlled. A further complication to the compounding and fabrication is the sensitivity of the conductive system to the work history. Generally, high and prolonged shear tends to degrade the conductivity of the system. Further, materials selection must be made with care to assure polymer reinforcement rather than mechanical property degradation.

Several of the resin compounders contacted can tailor the conductivity of the resin to fit the application. RTP Company, Wilson-Fiberfil International, and LNP Corporation all supply tailored conductive thermoplastic resins. This tailoring often results in a higher price/lb. Candidate materials which have been previously compounded with conductive fillers include PEEK, PPS, polysulfones, nylons, polyether sulfones, polyetherimides, PBTs, and the liquid crystal polymer. See Appendix for more information.

Physical Properties. In addition to the required electrical resistivity and mechanical properties, the material for use in the SDT also should have a number of desired physical properties. These include resistance

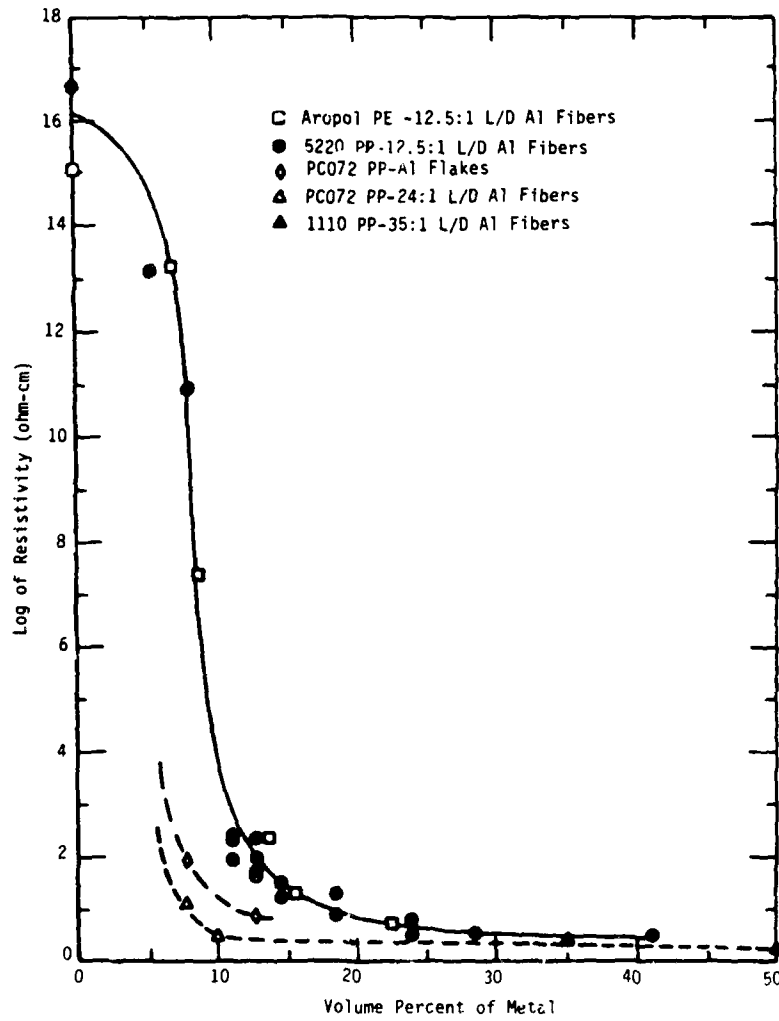
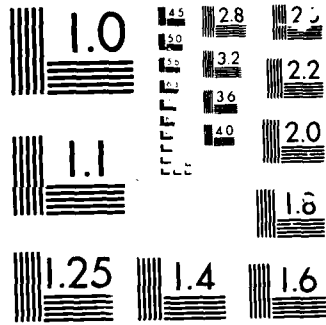


FIGURE 4.1. ADJUSTING CONDUCTIVE FILLERS TO ACHIEVE A SEMICONDUCTIVE SYSTEM



to various chemical and environmental factors, such as the cleaning agents, solvents, automobile/aircraft fluids, foods, beverages, and personal grooming items which may come in contact with the Data Tag.

There are several ways in which these environmental factors could affect the SDT. These include absorption of either water or saline systems which can change the electrical conductivity. Another potential effect is that of inducing environmental stress cracking in response to the residual molding stresses. Accordingly, the SDT molding system should have a low equilibrium moisture absorption and should be an environmental stress crack resistant (ESCR) grade. This accordingly mandates a high molecular weight polymeric engineering grade material which tends to have a high melt viscosity. Highly viscous systems can, however, cause incomplete fill, poor mold replication, as well as poor welding at knit lines, even at the high pressures required for injection molding.

Crystalline polymers generally are good candidate materials for applications requiring environmental resistance and good molding properties. These have good flow characteristics above the crystalline melting point. Such materials, however, may require imposition of a closely controlled molding temperature cycle if optimum crystallinity and physical properties are desired.

Thermal expansion properties also are critical, both with respect to part dimension control as well as minimizing residual stresses in the SDT. Products with high residual molding stresses are more subject to fracture after cooling, environmental stress cracking (ESC), and circuitry damage. Since polymers generally have high thermal expansion characteristics, the addition of a filler/reinforcement to reduce the thermal expansion properties may be necessary.

Finally, it is desirable that the SDT have good high-temperature stability and be resistant to thermally induced warping. Such properties as well as fire resistance are considered vital to the desired performance and service life of the unit. Based on the flammability resistance requirement of V-0, polyacetal was eliminated from the list of candidates, because it did not meet this requirement and is only able to reach a HB rating with the addition of flame retardants.

Physical properties of a potting system which have been shown to be acceptable in similar Datakey products are summarized in Table 4.6. Several compounders of electrically conductive resin systems were surveyed for possible candidate materials. Although the majority of these systems are designed for EMI shielding/static discharge, several options are possible:

1. The compounder can reduce the conductive filler to a level suitable for this application.
2. A nonconductive glass reinforced molding compound with the same base resin can be dry blended with the conductive system to provide the desired level of resistivity.

TABLE 4.6. PHYSICAL CHARACTERISTICS FOR RYTON SDT ENCAPSULANT

Molding Shrinkage, in/in, 1/8" section	0.0015	D-955
1/4" section	0.0025	
Water Absorption, % 24 hours at 23 C	0.02	D-570
Flammability, in/min.	SE	D-635
Flammability	V0	UL94

It should be noted, however, that the majority of these conductive systems are based upon chopped carbon fiber conductive filler. Accordingly, it will be necessary under either option to demonstrate the acceptability of a fibrous conductive element as opposed to the presently specified glass reinforced resin containing conductive carbon black.

A tabulation is presented of several potential molding systems, Table 4.4. These, along with the exception of the presently used system 1, generally are too conductive. Mechanical properties would appear to be satisfactory. Mold shrinkage is somewhat excessive, but compensation can be effected by using a glass fiber reinforced blend to adjust conductivity.

4.2.3.2 Survivability. Survivability of the SDT is based not only on the mechanical and physical and electrical properties, but the following considerations must also be made. How is the tag affected by:

1. Warfare and common chemicals
2. Nuclear radiation
3. Electromagnetic radiation
4. Microwave radiation.

Each of these factors will be discussed in greater detail below.

Chemical Warfare and Common Chemical Resistance. Important factors in the survivability of the SDT is the resistance to chemical and biological warfare materials, as well as common chemical agents.

Chemical Warfare Agents. Battelle's review of the current literature on polymeric materials has revealed that the effect of contamination has not been determined for many of the candidate thermoplastic polymers for the SDT. However, several possibilities exist:

- The agent has no effect on the SDT encasement and can be decontaminated and immediately reused in a clean environment
- The polymeric encasement could absorb the agent and later desorb life threatening concentrations
- The polymeric material could absorb the agent, causing structural changes--for example, swelling or softening of the resin--and render it unusable.

For these reasons, the susceptibility of the candidate materials to agents such as soman (GD), mustard (HD), and VX must be carefully examined. Theoretical correlations can be drawn between the polymeric material's permeability, solubility, and resistance to common solvents which have similar permeability parameters to warfare agents. From these correlations the chemical vulnerability of these polymers can be predicted.

A more direct and accurate method of determining the effect of chemical agents on polymeric materials is to perform actual laboratory exposures to agents. Not only the agent's effect on mechanical properties could be measured, but also the thermodynamics and kinetics of the agent penetration can be determined. The ability of a polymer and the SDT package to be decontaminated could also be examined. Decontaminating Solution #2

(DS-2), Super Tropical Bleach (STB), High Test Hypochlorite (HTH), and sodium carbonate are common decontaminating agents, and several are known to have detrimental effects on a variety of polymeric materials and possibly even to the metal contacts of the SDT. All of these various agents and decons would have to be examined to determine actual vulnerability of the tag.

Biological Warfare Agents. The biological threat is twofold: toxins and germs. However, the vulnerability of the SDT to biological agents is probably less than to chemical agents. Generally, the biological agents seek an environment conducive to growth, usually a living organism or a moist, warm area, preferably offering nutrients, for incubation. The most significant problem posed with biological agents is the carrier materials which are used to disseminate the toxins. These carriers may act as solvents of the SDT case and cause loss of mechanical or physical properties.

Another point to consider is that the vulnerability of the SDT to either chemical or biological agents is remote because the accessibility of the agent to the tag is limited. In a tactical environment the SDT would be inside the chemical protective overgarment, next to the body, which would protect the tag from exposure.

Common Chemical Resistance. Many of the problems associated with common chemicals, such as paint stripper, after shave, water, alcohol, etc., were discussed in the section on physical properties. However, most of the materials chosen as candidates for the SDT encasement have excellent acid, base, and solvent resistance. Examples of these materials and their resistance to various chemicals can be seen in Table 4.4.

Radiation Resistance. The energy of a nuclear explosion can be released by:

- An explosive blast, which is qualitatively similar to the blast from ordinary chemical explosions
- Direct nuclear radiation
- Direct thermal radiation
- Pulses of electromagnetic energy (EMP).

The nuclear blast usually drives air away from the site of the explosion, producing sudden changes in air pressure (e.g., static overpressure, which can crush objects, and dynamic pressure that results in high winds). Changes in pressure as a result of a nuclear blast would probably not affect the function of the SDT, even if the tag was in close proximity to the blast. However, the remaining effects of a nuclear explosion--direct nuclear radiation, thermal radiation, and EMP--would probably have a detrimental effect on the tag operation.

Discussion will first be confined to ionizing radiation, and to energetic subatomic particles (such as electrons, neutrons, protons, and alpha particles). Such particles have sufficient energy to ionize the medium through which they pass. Data has shown that much of the information developed in studying ionizing radiation is also applicable to UV radiation effects.

In general, ionized and excited molecules can cause crosslinking and molecular scission, and produce gaseous products. Crosslinking usually causes the polymer to become brittle and easily fractured. Scission, however, will degrade the chemical integrity of the polymer and loss of strength is noticed. An advantage of the crystalline, rigid polymeric material is that research has shown that crosslinking and scission induced by radiation will alter the properties of an amorphous, flexible polymer more rapidly than the properties of a crystalline material. However, the ability of a polymer to resist such an attack is dependent on the dose and flux density of the radiation, as well as the composition (including impurities) and the chemical structure of the polymer. Some gamma radiation resistance information on several of the most promising candidates can be found in Table 4.4.

Several general conclusions can be made concerning nuclear radiation.

1. Inorganic fillers such as asbestos and glass have greater degrees of ionic bonding than do organic materials and are less susceptible to bond breakage by excitation or ionization.
2. Aromatic groups tend to stabilize the polymer against radiation.
3. Halogenated compounds appear to be especially susceptible to radiation attack.

Electromagnetic pulse (EMP) is another way the SDT can be damaged by a nuclear detonation. EMP creates higher electric field strengths than radio waves, but it is a single pulse of energy that disappears in a fraction of a second (similar to lightning). The most common result of EMP would be the shorting of a capacitor or burnout of a transistor located on the IC chip. Although EMP would pose no threat to the encasement material, the unprotected microchip may be susceptible to transient radiation effects on electronics (TREE).

In a 3/23/84 report from Harry Diamond Laboratories, Nuclear Weapons Effects Division, it was experimentally shown that the prototype SDT can withstand repeated EMP threats of 50 kV/m. The Tag Interface Device experienced intermittent operation during exposure to the threat, but was not permanently damaged.

EMI Shielding. Although EMI shielding undoubtedly is desirable for chip protection, it is considered unlikely that the semiconductive encasement will be adequate. Its specified resistivity range of 10^7 to 10^9 ohm-cm is a much lower conductivity than is generally required for satisfactory EMI shielding. Generally, shielding properties require conductivities around 10^1 to 10^0 , as shown in the following discussion. (As a point of reference, wrapping the device in household aluminum foil would provide conductivities on the order of 10^{-1} , and would therefore not offer enough protection by at least one order of magnitude.)

Shielding studies are reported by Bigg and Bradbury for carbon black and nickel coated glass fiber composites. Three levels of Vulcan XC-72 conductive carbon black were hot milled into polycarbonate and molded into test plaques. The nickel coated fibers were dry blended with polycarbonate pellets prior to injection molding the test plaques. Resistivity values for these systems are shown in Table 4.7.

It should be noted that the conductivities of these composite polymer systems are considerably greater (7 to 9 orders of magnitude) than those of the current encasement material. Shielding values of the molded plaques were measured in the device shown in Figure 4.2. Effectiveness of these EMI shielding systems is shown in Figure 4.3a and b.

TABLE 4.7. ELECTRICAL RESISTIVITY OF POLYCARBONATE COMPOSITES

Filler	Volume Loading, percent	Resistivity, ohm-cm
Vulcan XC-72 carbon black	11	11.0
Vulcan XC-72 carbon black	21	3.5
Vulcan XC-72 carbon black	32	2.0
Nickel coated glass fibers	43	1.0

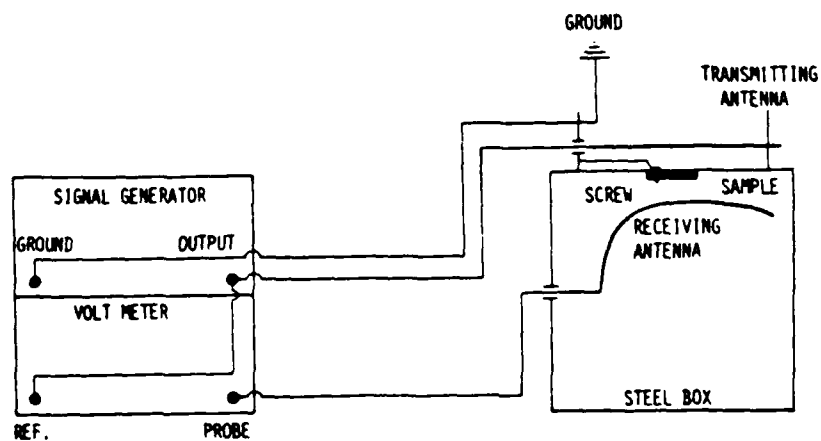
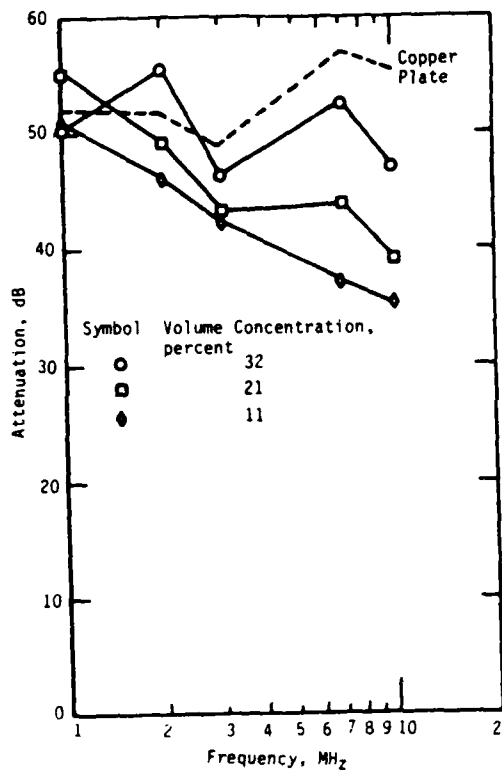
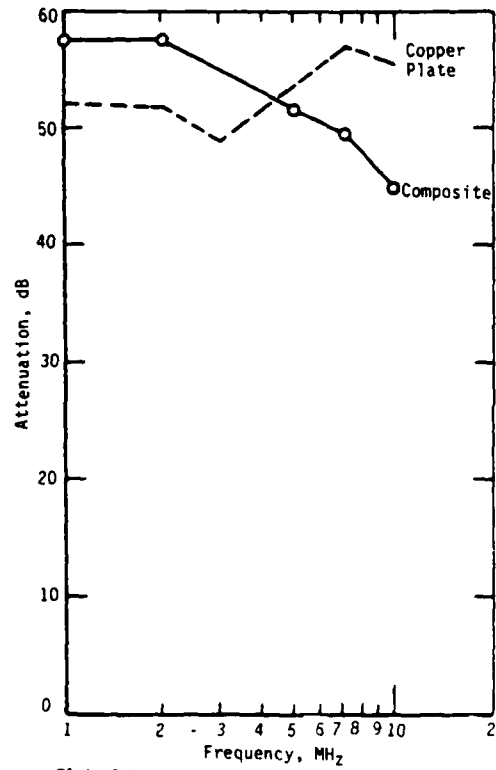


FIGURE 4.2. DEVICE FOR MEASURING SHIELDING VALUES

FIGURE 4.3a and b. EFFECTIVENESS OF EMI SHIELDING



Vulcan XC-72 carbon black



Shielding effectiveness of a nickel coated glass fiber-polycarbonate composite. Fiber concentration is 43 volume percent.

It is obvious from these results that an alternate approach must be taken to provide EMI protection for the SDT. Since most of the Data Tag dimensions are already fixed, a secondary encapsulation with a more conductive system will be difficult to implement. Further, this shielding system must not touch the contacts area or the system will short out. Additionally, this leaves an unprotected area. **It is believed that the most easily implemented EMI shielding system would be a conductive case.** Light weight metal enclosure concepts undoubtedly could be devised to provide the EMI shielding protection without affecting the functionality of the Data Tag. (See microwave resistance Figure 4.4a and b).

Microwave Resistance. Through discussions with Datakey, it became apparent that the microchip was not resistant to microwave radiation. **Because of the nature and makeup of the SDT, it is unlikely that the conductivity of the polymeric encasement can be made sufficient to shield against microwave radiation.** In order to be an effective shield, the polymer should have a conductivity range between 1 to 10 ohms. An encasement in this conductivity would cause the loss of stored data on the data chip.

One way microwave attack can be circumvented is by attaching a conductive case to the rivet already present to attach the chain to pass through the tag. When the soldier is in a potential microwave field the case can be worn over the SDT. When the tag needs to be read or written to, the case can be pivoted 180 degrees, as shown in Figure 4.4a and b. The case can be fashioned from a conductive composite which has the correct shielding conductivity. Even if the case is contaminated with chemical agent, it could be removed and a replacement case be put on. This should save the expense of replacing the tag.

The Army has experimented with one of Battelle's recommendations (see Figure 4.4) regarding tag shielding and has fashioned an SDT shielded by riveting two conventional metal ID tags to the SDT surface. While the above discussion regarding a disposable shield is true for the slip-on case, a riveted case could not be easily removed and replaced.

The use of an external case should make the SDT more resistant to both microwave and electromagnetic radiation. The design as shown in Figure 4.4b would also protect the SDT contacts from dirt, and could be fashioned with a low-grade magnet to prevent the box from unnecessarily opening.

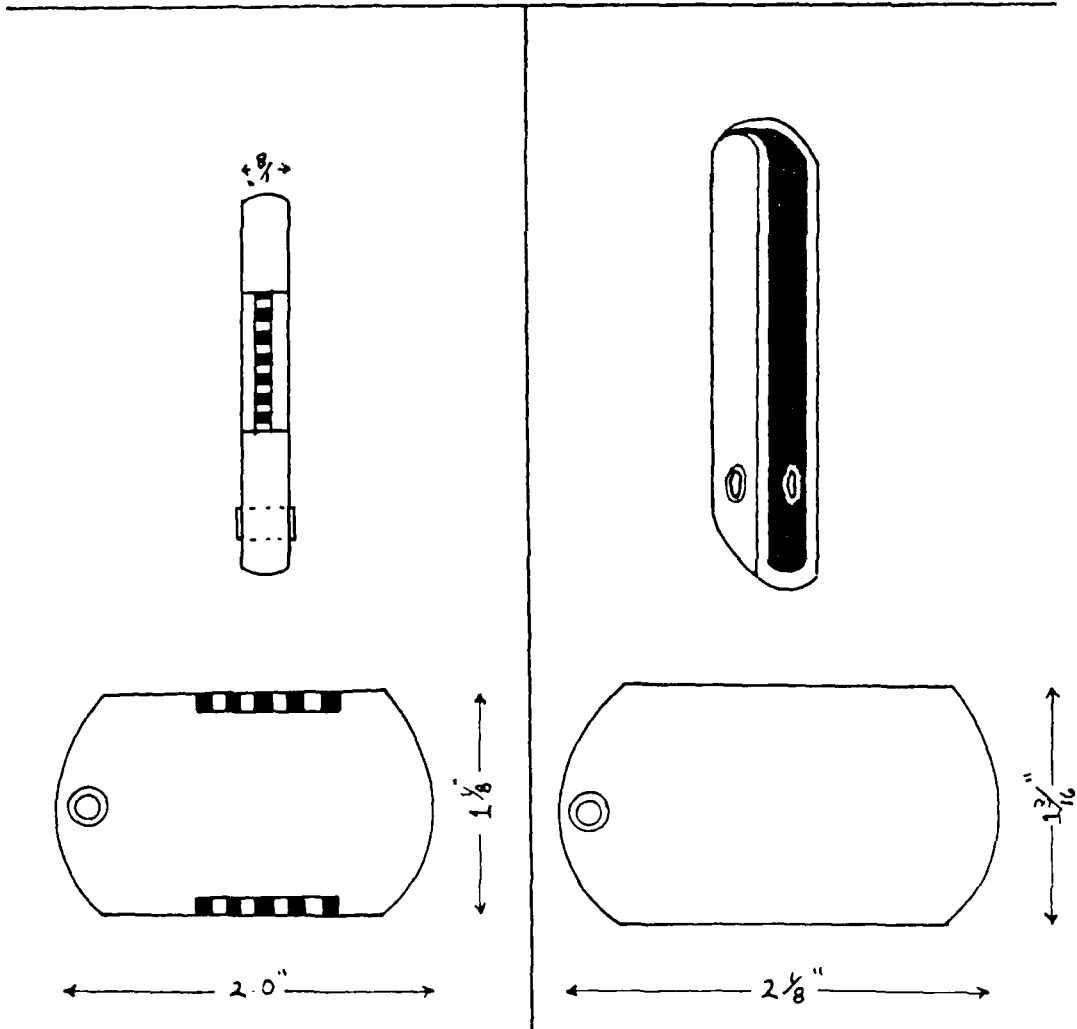
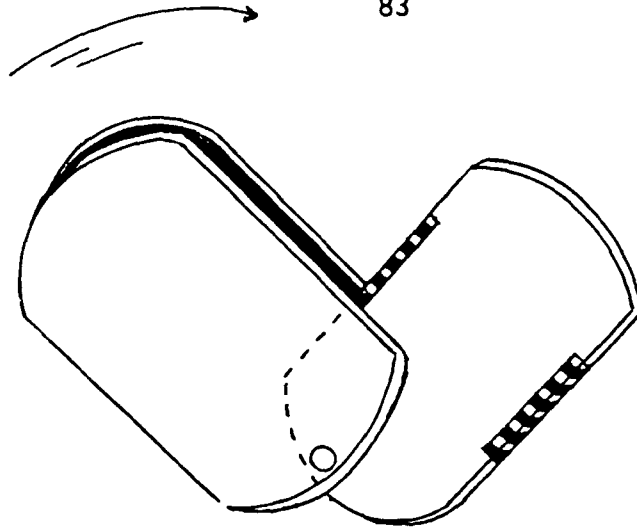


FIGURE 4.4a. POTENTIAL SHIELDING CONCEPTS FOR THE SDT

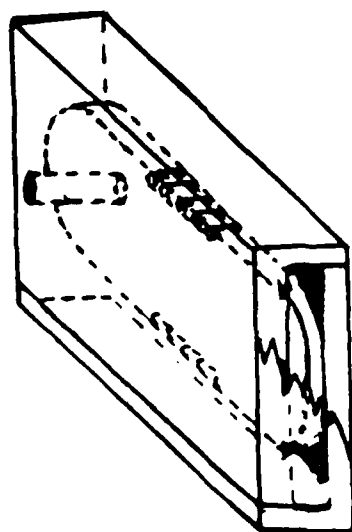
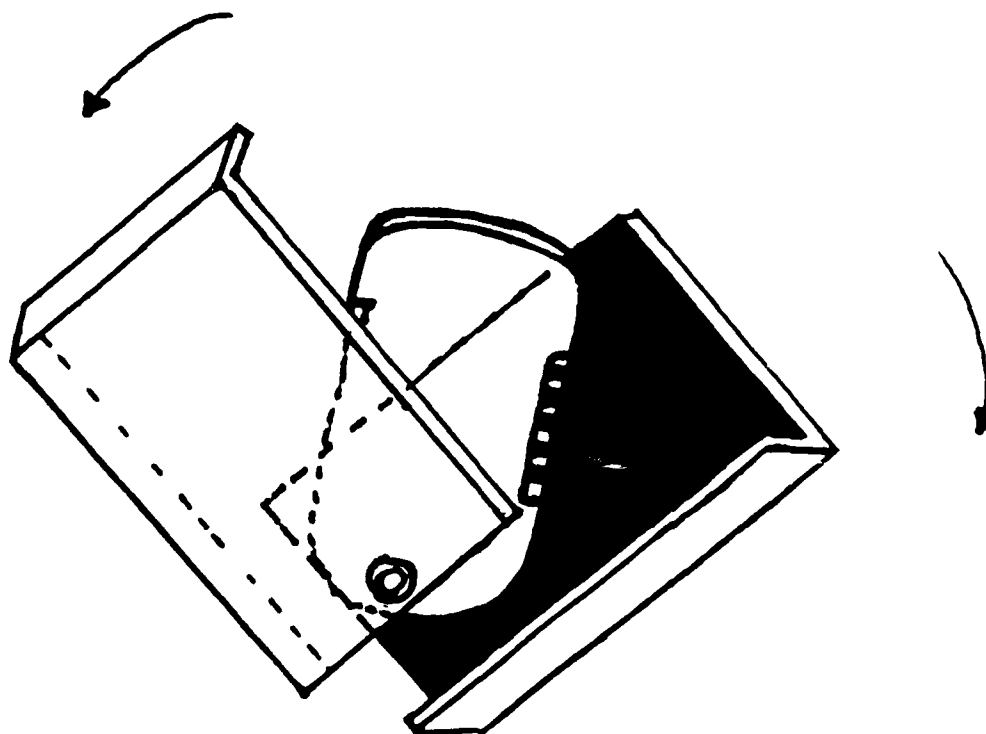


FIGURE 4.4b. POTENTIAL SHIELDING CONCEPTS FOR THE SDT

4.2.4 Surface Information

Previous discussions have referred to a tag with surface information. This subsection describes a variety of methods for accomplishing this feature. There are three major methods that can be employed to apply surface information to the SDT. These methods include:

1. Etching
 - a. mechanical
 - b. chemical
 - c. heat
2. Lamination
3. Printing.

Factors that will influence the implementation of these techniques include:

1. Is the surface information durable?
2. Is the equipment mobile?
3. How intricate can the surface information be (can it apply alphanumeric data, fingerprint, photograph)?
4. What is the cost?

Each candidate method and considerations will be discussed below.

4.2.4.1 Etching. There are three types of etching processes used for plastics: chemical, mechanical, and thermal. Chemical etching usually involves roughening the polymeric surface by a strong acid or alkaline chemical to ready the surface for coating or printing. Phosphoric or chromic acids or permanganate solutions are the most common etching materials used. Etching solutions usually work by attacking the amorphous entity of the polymer rather than the crystalline portion. Chemical etching is best suited for a large area rather than etching an intricate design. However, the chemicals can be carried in small containers and are, therefore, quite mobile for field use. The materials, however, are quite corrosive and may need to be stored in glass rather than plastic containers, which may pose a shipping problem. The

chemicals for etching are inexpensive, but usually etching is only the first step before an additional printing technique takes place.

Mechanical etching can include the use of hand tools or automated tools. Although the hand tools are easily mobile, the speed, accuracy, and efficiency in producing surface information on a data tag is operator/manual dependent. Simple lettering is probably the only type of surface information which can be applied with a hand tool. For this reason, manual etching would probably not be a method of choice.

Automated equipment includes mechanical engravers (like the manual operations but manipulated automatically) and lasers. The mechanical engraving equipment would have the same limitations with respect to the types of information that could be encoded on the tag.

Thermally, lasers have been used for etching simple as well as intricate designs on plastics. Etchings, through the use of laser technology, are durable and can be used for applying all types of surface information. However, the cost of the equipment is high and it may be cumbersome when being moved to the field.

4.2.4.2 Lamination. Lamination is a fairly simple technique which can easily be used in the field to apply surface information. Most probably lamination would be used in conjunction with some reverse-printing techniques and would serve to protect the printing from abrasion. Adhesion of the laminate to the SDT would not be an extremely critical parameter since the process is inexpensive and the laminate can readily be reapplied in the field. Methods of printing the lamination films are described in the following sections.

4.2.4.3 Printing. There are a number of printing techniques that are used to apply information to various substrates. The most common methods include:

1. Letterpress
2. Flexography
3. Lithography

4. Gravure
5. Thermal transfer printing
6. Ink-jet
7. Electrophotography.

However, these printing techniques would not apply a durable coating which has abrasion and chemical resistance. Therefore, these methods may need to be used in conjunction with lamination or overcoating.

Letterpress, flexography, lithography, and gravure printing all require a printing plate, cylinder, or roll to carry the information to be printed. Therefore, these techniques may not be directly amenable for field use. Since a different plate would be needed for each tag that was to be printed in the field, a large number of plates, along with the proper etching materials, also need to be carried along. As a result, these techniques would be complex, time consuming, and cumbersome. However, the techniques might be used to "preprint" a lamination film or other substrate that could be used in the field to transfer information to the SDT.

Thermal transfer printing is another method that can be used to apply surface information to the SDT. The information is transferred from a carrier to a receiver substrate (the SDT) by heating localized areas of the carrier. Characteristics of this printing include an electronic output (such as to a computer), and a resolution of 200 lines per inch (LPI). Technology is currently trying to attain 400 LPI. Another embodiment of the thermal transfer process involves the preprinting of a carrier web with the desired information using a special subliminal ink or dye. When the SDT was prepared in the field a section of the preprinted substrate would be heated in contact with the SDT and the information transferred by sublimation. The size, mobility, and cost of this type of equipment and application is uncertain at this time.

Ink-jet printing is a technology that can be easily adapted for use with the SDT. This printing involves depositing droplets of ink onto a surface in a controlled manner to form an image. Droplets are generated in response to an electronic input obtained from scanning an original document or

image, or directly from electronic storage media. There are three methods of ink-jet printing:

1. Continuous drop
2. Drop on demand
3. Intermittent.

Resolution from this type of printing is in the range of 250 LPI.

Most likely the drops would have to be applied as a reverse print to a film and finally laminated to the SDT. Size, mobility, and cost of this type of equipment, depending on the resolution and information images required, could be amenable for field usage.

A final method of applying surface information is by using electro-photography techniques. This technology may require additional research to suitably fit it to the requirements for the SDT. However, when the technology is utilized, it will provide a small, mobile unit which should prove quite cost effective.

This technology is similar to xerography in that a charge is deposited in selected areas of a dielectric layer and then the charged areas are developed with either dry or liquid toner. The resolution of this type of printer is 200-240 LPI.

Since the SDT is a conductive-type plastic (to minimize electrostatic and other problems), the information images will need to be formed and developed on a separate belt or carrier, then transferred to the SDT, and the toner image fused by heat. The technique could also be used to image a lamination film as well.

This technology can easily be used to apply alphanumerics to the SDT. Depending on the resolution required, the application of a fingerprint and a photo need to be demonstrated.

There are several problems associated with coating plastics. A few of these include:

1. Adhesion of the images to the SDT
2. Humidity effects on the imaging process
3. Image resolution required (i.e., will the images involve alphanumerics, fingerprints, photographs, and/or combinations?)

Therefore, candidate printing techniques, the imaging material (ink or toner), and the final format (direct image or lamination) should be studied further, both conceptually and experimentally, to identify the best overall system for field usage with the SDT.

Additional printing techniques considered but not discussed herein because they were judged inappropriate for the desired application include:

1. Screen printing
2. Hot stamping
3. Conventional electrostatic spray
4. Valley printing.

Table 4.8 describes major points concerning these application techniques. It should be noted that in addition to the automated printing techniques mentioned above, it may also be possible to manually "write" information onto the tag using marking pen technology. An epoxy-based ink has recently been developed which could be suitable for this approach.

4.2.5 Conclusions

From the summary (Table 4.9) it can be seen that the following materials would be inappropriate for the SDT application.

- (1) Diallylphthates - thermoset, therefore, cannot reuse scrap; needs additional additives to obtain a UL-V-0.
- (2) Fluoropolymers - difficult to process; corrosive to the equipment, expensive.
- (3) Nylons - high moisture absorption which can affect properties (especially nylon 6 and 6/6), UV sensitive; limited acid and base resistance.
- (4) Polyetheretherketones - expensive; cost does not justify the excellent properties.
- (5) Phenolics - thermoset; therefore, cannot reuse scrap; poor resistance to alkalis.
- (6) Polyacetals - UV sensitive, UL94 - V-0 cannot be achieved even with additives; poor resistance to strong acids and bases; therefore, could not be decontaminated easily.

TABLE 4.8. PRINTING TECHNIQUES INAPPROPRIATE FOR SDT APPLICATIONS

Process	Operation	Equipment	Applications	Effect
Screen Printing	Ink is applied through a finely woven screen. Screen masked in areas where no paint is needed.	Screens, fixtures, squeeze, press set-up dryers. Manual operation is possible.	Bottles; large application areas.	Single or multiple colors; time consuming.
Hot Stamping	Transferring coating from a part by pressure/heat. Impression is made by metal or silicone die. DRY PROCESS.	Rotary or reciprocating hot stamp press. High speed.	Can not easily print on round or curved surfaces.	Foil can be specially formulated. Equipment may be difficult to move.
Conventional Spray	Spray by air or airless gun.	Spray guns and booth dryers.	Some materials may require surface treatments.	Covers large areas and uneven surfaces but not in image patterns.
Electrostatic Spray	Charged particles sprayed electrically on conductive parts; high paint utilization. More expensive than conventional spray.	Spray gun; high voltage supply; pumps; dryers.	Used for all plastics.	Good over all coating but not for defined image patterns.
Valley Printing	Uses embossing rollers to print depressed areas.	Embossor with metal image plates ink attachment.	Used for floor tiles, upholstery.	Generally two color maximum.

TABLE 4.9. ADVANTAGES AND DISADVANTAGES OF CANDIDATE MATERIALS

Polymer	Advantages	Disadvantages
<u>Allylphthalates</u>		
Thermoset		
Thermal	Excellent heat resistance.	Needs additives to obtain UL-V0.
Mechanical	Low creep, excellent mechanical properties. Abrasion resistant.	
Chemical	Good chemical resistance.	
Other	Inexpensive.	Can not reuse scrap.
<u>Fluoropolymers</u>		
Crystalline/Thermoplastic		
Thermal	Continuous thermal capability to 400°F, some to 500°F. Fire resistant.	Can emit halogen compounds, if burned.
Mechanical	Tough, flexible, high impact strength.	Difficult to process. Low tensile and flexural strength. Low creep resistance.
Chemical	Inert to strong acids, bases, some organic solvents. No moisture absorption. UV stable.	Halogenated or aromatic materials may have some effect.
Other		Corrosive to processing equipment.

TABLE 4.9. (Continued)

Polymer	Advantages	Disadvantages
<u>Liquid Crystal Polymer (LCP)</u>		
Crystalline/Thermoplastic		
Thermal	High HDT. Low coefficient of thermal expansion.	
Mechanical	Low mold shrinkage self reinforcing-- leading to high strength and stiffness; impact resistant.	
Chemical	Resistant to strong acidic, oxidative, and basic chemicals.	
Other	Excellent low temperature properties.	Will not be commercial until April-May 1985.
<u>Nylons</u>		
Crystalline/Thermoplastic		
Thermal	Glass reinforced retains high strength at high temperatures and decreases coefficient of thermal expansion.	
Mechanical	Tough, impact resistant; excellent fatigue resistance. Nylon 6/6 high tensile strength and flexural modulus. Nylon 6/12, 11, 12 have better dimensional stability.	

TABLE 4.9. (Continued)

Polymer	Advantages	Disadvantages
<u>Nylons (Continued)</u>		
Chemical	Resists aromatic, chlorinated and ketone solvents, gasoline, and oil. Good abrasion resistance.	Properties affected by moisture absorption (especially Nylon 6 and 6/6). UV sensitive. Limited acid resistance. Only satisfactory in resistance to mild and moderate base solutions.
Other	FDA approved.	
<u>Polyetheretherketones</u>		
Crystalline/Thermoplastic		
Thermal	High temperature resistance. Suitable for applications to up 600°F. Service life 50,000 hours at 450°F.	
Mechanical	Tough, strong, rigid. Resistant to abrasion and fatigue.	
Chemical	Excellent acid and base resistance. No organic solvent attack has been observed on molded parts.	
Other	Radiation resistant to 1100 Mrads without significant degradation.	Expensive.
<u>Phenolics</u>		
Thermoset		
Thermal	Excellent heat resistance. Low coefficient of thermal expansion, UL94, V-0.	

TABLE 4.9. (Continued)

Polymer	Advantages	Disadvantages
<u>Phenolics (Continued)</u>		
Mechanical	Low mold shrinkage, low creep. Excellent dimensional stability, toughness, surface hardness.	
Chemical	Excellent resistance against weak acids. Good resistance against strong acids.	Poor resistance to alkalis.
Other		Can not reuse scrap.
<u>Polyacetals</u>		
Crystalline/Thermoplastic		
Thermal	Fillers improve HDT's. Good thermal properties. Coefficient of thermal expansion similar to metals.	UL94, V-0 can not be achieved even with additives.
Mechanical	Tough, excellent creep resistance. Performance equals metal.	
Chemical	Moisture absorption does not affect properties, except at elevated temperatures.	Poor resistance to strong acids and bases. UV susceptible, needs absorbers to improve outdoor longevity.
Other		Water >180°F and steam will have detrimental effects.

TABLE 4.9. (Continued)

Polymer	Advantages	Disadvantages
<u>Polyamide-imides</u>		
Amorphous/Thermoplastic		
Thermal	High HDT's and continuous service temperature. Coefficient of thermal expansion similar to metals when reinforced.	
Mechanical	Tensile, flexural and impact strength retained at high temperatures. Low creep. Stress crack resistant.	
Chemical	Unaffected by aliphatic or aromatic hydrocarbons, chlorinated solvents and most acids and bases.	Water absorption causes swelling and affects properties.
Other		Expensive.
<u>Polyarylsulfones</u>		
Amorphous/Thermoplastic		
Thermal	Higher HDT than polysulfone or polyether sulfone. High continuous service temperature.	
Mechanical	Tough, good creep resistance. Notch sensitive.	
Chemical	Resistant to fungus, hot water and steam. Resistant to common acids and bases.	Affected by esters, ketones, and aromatic hydrocarbons.
Other		

TABLE 4.9. (Continued)

Polymer	Advantages	Disadvantages
<u>PBT/PEI</u>		
Crystalline/Thermoplastic		
Thermal	Good dimensional stability at elevated temperatures. Low coefficient of thermal expansion.	
Mechanical	Stiff, high tensiles and flexural strength, tough, low warp and high impact grades available. Excellent moldability.	
Chemical	Low moisture absorption; resists most solvents at R.T.	Poor resistance to strong alkalis.
Other		
<u>Polyetherimides</u>		
Crystalline/Thermoplastic		
Thermal	Retains physical, mechanical and electrical properties after long exposure to elevated temperatures; coefficient of thermal expansion equal to metal.	
Mechanical	High tensile, flexural and impact strength. High creep resistance. Low friction and wear.	
Chemical	Resists most organic solvents.	Attacked by alkalis and concentrated inorganic acids.
Other		

TABLE 4.9. (Continued)

Polymer	Advantages	Disadvantages
<u>Polyethersulfones</u>		
Amorphous/Thermoplastic		
Thermal	Retains strength for long use at 400°F. Low coefficient of thermal expansion. Low smoke emissions.	
Mechanical	Tough, good creep resistance.	Notch sensitive; improved by glass reinforcement.
Chemical	Good resistance to aqueous acids and bases and some organic solvents.	Affected by esters, ketones, methylene chloride and polar aromatic solvents.
Other		
<u>Polyphenylene Sulfide</u>		
Crystalline/Thermoplastic		
Thermal	Retains mechanical properties to 500°F. Low thermal expansion; good long-term thermal aging characteristics.	
Mechanical	High stiffness and strength. Low creep.	
Chemical	No known solvents under 400°F. Excellent chemical resistance to 200°F. Low water absorption.	Poor resistance in oxidizing environment >200°F.
Other		Corrosive to processing equipment.

TABLE 4.9. (Continued)

Polymer	Advantages	Disadvantages
<u>Polysulfone</u>		
Amorphous/Thermoplastic		
Thermal	High HDT's and continuous service temperature. Retains mechanical properties to 350°F.	
Mechanical	Low creep and mold shrinkage. Good impact strength.	Notch sensitive.
Chemical	Resistant to fungus, mineral acids, alkali, and salt solutions.	Poor resistance to polar organic solvents, like ketones, esters, and aromatic hydrocarbons.
Other	FDA approved.	UV sensitive.

- (7) Polyamide-imides - water absorption can affect properties; expensive.
- (8) Polyarylsulfones - affected by various solvents containing ketones, esters, and aromatic hydrocarbons.
- (9) Polybutylene terephthalate/polyethylene terephthalate - not easily decontaminated; attacked by strong acids and bases.
- (10) Polyetherimides - attacked by alkalies and concentrated inorganic acids.
- (11) Polyethersulfones - affected by ketones, esters, methylene chloride, and polar aromatic solvents; notch sensitive.
- (12) Polysulfone - affected by ketones, esters, and aromatic solvents; notch sensitive, UV sensitive.

It is the project team's conclusion that polyphenylene sulfide (PPS) and liquid crystal polymer (LCP) are the best materials for the manufacture of the SDT.

From the data previously presented, the following conclusions can be made:

- (1) Mechanical properties for the SDT are less critical requirements than electrical, physical, and chemical properties.
- (2) Based on physical, chemical, and processing requirements; two polymeric materials, polyphenylenesulfide (PPS) and liquid crystal polymer (LCP), are viable candidates of the SDT encapsulating material. Both of these materials cost between \$6.50 and \$7.50 per pound.
- (3) Processing equipment life will be diminished by at least half, and utility costs will double with the use of PPS. However, estimated total unit costs for the PPS is only 4 cents more than for the LCP.

4.3 Tag Interface Device Design Issues

Although the tag is the central component of the SDT system, the Tag Interface Device (TID) performs the critical function of interfacing the tag to the rest of the ADP world. Without referring to specific implementation

decisions, the TID can best be described in terms of its functional components: tag interface, host interface, display, and (optionally) input. At this level of abstraction the overall function is simple; as various design issues are added the picture becomes more complex.

In this section are discussions of the following issues:

- TID performance requirements
- Impact of tag technology selection
- TID software issues
- Alternative communication methods
- Conclusions.

The discussion of alternative communication methods has relevance to the tag design as well as the TID design. It is included in this section because of its potential impact on both software and host machine requirements.

The importance of a system-level viewpoint during selection of the tag technology and design cannot be overemphasized. The tag technology selection almost completely drives the technology and design of the tag interface device.

Although there are at least four identifiable component functions in the tag interface device, the tag interface is the dominant technological issue.

The TID is as critical an item to success of the system as the tag with respect to its cost and performance. Use of the SDT system depends on the widespread availability of TIDs. If they are unavailable either because their cost prohibits adequate supplies or because of reliability problems, the system is useless.

The TID must exhibit acceptable levels of performance in each of the following:

- (1) **Availability** - must use currently available technologies; would like currently available components if possible.
- (2) **Reliability/Survivability** - must perform for extended periods under adverse conditions; expected life is 10 years.

- (3) **Size and Weight** - must be small enough and light enough to avoid posing a transportation burden even at the level of being carried by an individual. This restriction must include the device's power supply if separate from that of a host ADP machine.
- (4) **Cost** - the cost of the device must be low enough to avoid inhibiting its availability.
- (5) **Maintainability** - must pose no requirements for maintenance which cannot be fulfilled by current VIABLE/TACCS operator personnel.

The two major candidates for the tag technology, digital electronics and optical stripe, differ radically in their impact on TID design. So different are the two that an item-by-item comparison is possible only on the level of the performance measures stated above.

A digital electronics based tag must be provided a small amount of electrical power, and (several) two-way logic-level information paths. While the simplest and cheapest approach is to use mechanical contacts, these exhibit some reliability problems under prolonged exposure to unfavorable conditions. Noncontact alternatives are discussed in detail later in this report. Although some of them are more complex than simple contacts, all are capable of being manufactured with current technologies. They also would allow the size and weight of the TID to approach that of the tag itself.

Optical stripe technology tags require an interface built around a laser. Current laser diodes may not be adequate for the task, so this requirement could place a rather uncomfortable limit on the best size, weight, cost, reliability, and maintainability of the TID.

Other components of the TID, such as the indicator and cables, follow more conventional patterns and are not discussed here. Two issues which will be covered in more detail are possible methods for noncontact connection to electronic tags, and software issues for TID control and communication with the host.

4.3.1 TID Software Issues

In the early 1960's, hardware represented 90 percent of ADP costs. Today, it represents 20 percent, with 80 percent going to software and

software maintenance. By 1990, experts predict that software will increase to 90 percent of system costs. Therefore, it is important to examine the aspects of TID software for the SDT system.

Use of microcomputer control in the TID can safely be assumed; it is the only way to achieve the required flexibility. It does, however, raise some important issues for both the design and post-deployment support of the SDT system. Software will be involved in three critical TID functions: tag interface, host interface, and data manipulation. Each of these will be described in the following section. After that, problems specific to each function will be identified, along with approaches to solve or avoid them.

Functions of Software in the TID. Specific functions of the tag interface depend strongly on the technology and design chosen for the tag itself, but they can be expected to include various data transfer operations and monitoring of the interface equipment's operation. Additional operations may include error checking and recovery, and implementations of security functions. This will be a relatively stable function; once the system design is frozen the requirements for the software won't change.

Interface to a host ADP machine is a critical design issue. Most of these machines have been designed and built with no provisions for attaching auxiliary devices other than an occasional printer. Connection in any form may be difficult, and application-transparent connection much more so. This function is most likely to take the form of a communications protocol. Design of this protocol is a separate issue from the software to implement it, and it is crucial for robust system performance.

Data manipulation functions involve some of the currently least-defined operations. This is due primarily to their application-specific nature, and the fact that most of the SDT system's eventual applications haven't been identified yet. For any given application it can be assumed that both the specific data items required and the format, order, and encoding schemes of the items will be unique. They may also vary with design changes in the application. As long as the tags are used as alternate sources of information which would otherwise have come from a keyboard, and as repositories for information normally displayed on a terminal, the operations will be limited to reorganization. This is much more manageable than compression/

decompression operations, which require additional procedural and tabular information specific to the scheme being used.

Problems and Potential Solutions. For all the functions of software in the TID, one of the fundamental problems is programming "bugs". Regardless of the skill and effort applied to design, implementation, and testing, there is still always a possibility of errors not found until after the system is put into use. Field use by regular users can find bugs which months of testing will fail to identify.

Once a problem is identified, finding and correcting the program error is usually relatively simple. For software embedded in many independent devices scattered all over the world, the problem of publishing corrections can be overwhelming. The minimum design approach to allow program correction in the field is to store the code in a replaceable device such as a standard PROM IC. The socket for this IC can be uncovered by removing the TID case or, optionally, by removing a small panel provided for this purpose. The IC itself can be in an industry-standard package such as a DIP or QUIP, or it can be in a package such as those used to provide programs for programmable calculators. In any of these, program updates are published by manufacturing new memory devices with the corrected code stored in them, and distributing these to every holder of a TID. Either the regular user of the device or a maintenance crew member would replace the defective IC and dispose of it. A different approach is to store the code in erasable memory such as that under consideration for the tag. Program updates would be published by sending them through VIABLE or distributing them on magnetic media, then loading them into each TID upon first connection to a host. A small loader program would be permanently built in to facilitate this operation. This approach would have a faster turnaround than the others, and would also avoid the problems inherent with distributing and installing thousands of ICs.

The problem of program errors applies to all functions in the TID which depend on software. In the discussions which follow, additional problems specific to each function will be described under an assumption of program correctness, except where specifically stated. Overstating the strength of that assumption would be very difficult.

Tag Interface Functions. Perhaps the major issue involved in any discussion of the tag interface is reliability under adverse conditions. Hardware in both tag and TID must provide the basic performance required, but software could provide mechanisms for recovery in case of soft errors (noise-related, nonrepeating bit faults), or even partial failure of a tag. If the interface involves a communications protocol, it should have a mechanism for error correcting codes included in the design. For example, simple logic-level connections can be read three times and compared; all writes can be verified the same way.

Host Interface Functions. The exact role of software in this function depends on the overall approach selected to accomplish it, and therefore at this time the discussion of problems is very general in nature. It seems safe to assume that the interface will be some form of serial communications link, and can therefore be discussed in terms of layered protocols. However, even this simple item raises an issue which deserves separate discussion. This is the need for connection facilities designed into the host machines. Very little can be accomplished in the area of communications protocols if cooperating software on the other end can't be assumed, and physical connection is necessary but not sufficient. Only by using techniques like piggy-backing into existing communications lines can a totally noncooperating connection be made at all, and this can provide no benefits beyond access to low-level data streams. Examples of existing lines which may be available are the keyboard interface and the printer port, each of which is unidirectional. The keyboard line in particular is likely to be different among the various possible host machines, if not at the physical level then certainly by the message level protocol. The uncertainty and complexity this introduces to the system design may become prohibitive, particularly in the situation where more applications of the SDT system are desired. Only by assuming some degree of cooperation can the benefits of the following items be realized.

As a general rule, the lowest layer implemented in software should include error correction capabilities. System reliability will be greatly improved at low equipment and time cost. Equipment costs are limited to a few hundred bytes of storage for additional code; time costs to the calculation of checksums or other values and the occasional retransmission of a faulty message.

Data Manipulation Functions. By far the greatest source of operational problems for the SDT system is in the addition of new applications and changes in existing applications. Although reformatting information for a small number of different applications is a manageable task, the accumulation of requirements from an increasing number of applications could grow without bound. Some of the problems are similar to those encountered with publishing software corrections, and can benefit from the same approaches described for that. Other problems relate more to the sheer magnitude of the attempt to accommodate widely varying requirements in a device as small and inexpensive as the TID must be. **An approach which is superior in all technological respects is to make each application responsible for performing the translation between its own data format and that of the SDT system.** The latter would be specified as a fixed set of rules for locating and placing information in a tag, and implemented in the TID software. For example, an application which needed the soldier's name would send the TID a message indicating that it needs the name. The TID could respond with the name, in a fixed format, using methods completely unknown to either the host machine or the application software. This scheme can work very well and provide a great deal of flexibility, but it absolutely depends on the application sending the request message. Most present-day applications software uses the metaphor of filling in a fixed form as the basis of the user interface design. Often the code which controls this function resides in the terminal. It may be possible to replace this code which interrogates and reports to the TID in parallel with its normal operations with the screen and keyboard. Once again, this approach could work very well in the field but it absolutely depends on cooperation.

Barring any changes in the host machine or application software, the only way to accommodate varying applications is to make the TID software easily changeable. Suitably packaged memory ICs containing either entirely new code or tables of information specific to the application can be inserted in the TID prior to use. The operator of the host machine would be responsible for insuring that the proper IC was in place, since the host application and machine would need to know about TIDs to perform an automatic check.

4.3.2 Alternatives To Metallic Contacts

The current experiments with SDT systems have taken place using tags with metallic contacts. Based on the envisioned environment for tag use, it is possible that metallic contacts may prove to be unreliable. This section describes several alternative methods of transferring data into and out of the tag device.

The development of a Soldier Data Tag entails several design goals including resistance to a variety of environmental conditions, long life, and high survivability. The data must be able to withstand fire, water, fuel, corrosives, and sunlight as well as be resistant to electromagnetic radiation and chemical warfare agents. To this end, considerable emphasis has been placed on selecting the appropriate material and fabrication process that will encapsulate the microcircuitry and make the tag durable for military applications.

Resolving the issue of alternate packaging materials is a necessary step for developing an applications compatible and rugged SDT. Unfortunately, by design, the material cannot completely cover the circuitry it is intended to protect. Breaks in the protective surface must be incorporated to allow metallic electrical contacts to be brought to the surface of the tag. These contacts are required to directly couple power into the circuitry and permit digital communication with the embedded processor. The metallic surface will be subject to the same environmental conditions as the protective polymer and must have the same resistance capabilities. That is, the contacts cannot be subject to moisture- or solvent-generated corrosion, and they must ensure that a reliable interface can be established between the SDT reader and the tag itself.

Abrasion resistance, as measured by the number of insertions, is probably adequate for a 10 year life of the prototype tag. The metallic contacts are rated at 20,000 insertions by the manufacturer, which translates to 5 or 6 insertions per day over a 10 year life. **However, it is surface corrosion which actually dominates contact reliability.** Added thickness will not affect corrosion resistance.

The use of surface contacts presents other issues such as proper bonding between dissimilar materials in the fabrication process and the

drawbacks associated with direct electrical access to the tag's circuitry. Since both the metallic surface and the polymer surface comprise the total protective shell of the tag, the fabrication process must ensure that the polymer tightly seal against the metal. Any gapping between the two materials will represent areas of penetration for environmental factors to gain access to the internal electronics. A direct conducting path to tag's electronics provides a convenient and simple means of interfering with the tag; however, these same conducting paths also allow high voltage charge from electrostatic discharge to propagate and potentially destroy the circuitry through over-stress. Similarly, electromagnetic radiation can more easily be transferred to the embedded circuitry via the exposed electrical conductors. In short, direct electrical contact with the data tag may be simple, inexpensive, and convenient, but the presence of metallic surface contacts electrically connected to the circuitry may also be the tag's area of greatest vulnerability.

Completely eliminating the surface contacts entails a number of trade-offs. The data carrier's resistance to environmental influence can be maximized, since apertures need not be included in the structure of the encapsulating material. Since contact degradation would no longer be an issue, system reliability may be increased. And, if the tag can be constructed without distinguished surface features, an element of security can be added to the SDT system. However, these advantages are achieved at the cost of more complex and consequently more expensive circuitry in both the Soldier Data Tag and the tag interface device. In addition to the electronics used in the direct contact approach, alternate communication methods for a noncontact approach incorporate circuitry that allows the reader and the tag to communicate with each other and, perhaps, allows the tag's embedded circuitry to be powered without the use of metallic contacts.

4.3.2.1 Alternative Approaches. Several approaches are available for transferring electrical energy to and from the SDT without the use of external surface conductors. In each approach, an electrical signal is converted to another form of energy (other than flowing electrons), transmitted to the data carrier, and reconverted into an electrical signal. This process effectively transfers power and data into the tag; a similar process is used

to transmit data from the tag to the reader. From past experience the Battelle project team has found that there are basically three viable ways of establishing a noncontact interface in systems such as the Soldier Data Tag. They are: (1) electromagnetic, (2) optical, and (3) electromechanical. In the electromagnetic approach, electrical signals are converted into a form of electromagnetic radiation. Depending on the specific configuration, the energy is coupled using either magnetic induction, wave propagation, or magnetic Hall effect. In the optical approach digital data is converted into a series of light that are directed and converted into an electrical signal by a photoreceptor. And, in the electromechanical approach, signals are converted into an acoustic emission which is detected by an acoustic resonator. For some of the approaches, only data can be transmitted to and from the tag, and another noncontact approach must be used to couple power to the tag circuitry. But in all cases, direct electrical contact is eliminated from the reader/tag interface.

Presented in Table 4.10 are six different noncontact communication/power transfer technologies, in addition to direct contact, that may also have a use in the SDT system. While most of the technologies are relatively straightforward and use common design practices, the remaining technologies are simply conceptual designs based on some common electrical parameter function such as Hall effect voltage as a function of magnetic field strength. In general, the conceptual designs demand extensive development and refinement before they can be seriously considered for application to the SDT system. The list can be expanded by combining some of the technologies to make up for any limitations in the individual designs, but of course, compatibility between the technologies must be maintained. For example, an induction coil can be incorporated into the optical interface, which is not inherently self-powered, to provide power to the circuitry and optical components embedded with the tag. Some shielding may need to be added to protect the circuitry from induced voltages; however, the magnetic induction and optical coupling processes are each unaffected by the other and are, thus, mutually compatible.

The evaluation of the designs was a qualitative assessment based on several technical, economic, and applications-oriented criteria. The first, and most obvious, is technical feasibility, that is, the practicality of implementing the design for a SDT system. In general, those ideas that were

TABLE 4.10. COMMUNICATION/POWER TRANSFER TECHNOLOGIES

Specific Technology	Example of Use
Direct Contact	Memory Cards
Inductive Coupling	Implanted Heart Pacemakers
Radio Frequency Waves	Inventory Tags
Electromagnetic Waves	Inventory Tags
Magnetic Hall Effect	Position Sensors
Optical Coupling	Serial I/O Ports
Acoustic/Piezoelectric	Sonar

merely conceptual tended to score lower in this category than the already-implemented designs. Reliability is closely related to technical feasibility and is defined by both the ability to perform when necessary and the ability to perform without error. That is, the communication technique should not only respond when prompted, but it should faithfully and accurately transmit and assimilate the information being sent. Obviously, the reliability and performance of the SDT system largely hinges on that of the communication/information transfer interface.

The maintainability of the interface ultimately translates into an overhead cost to operate the system. In most cases, the cost of maintenance is dominated by personnel charges for periodic checking, and modules, the additional cost of batteries is also incurred.

The technologies were also assessed for their applicability to the rather rigorous environmental resistance design guidelines. The Soldier Data Tag must be able to withstand elevated temperatures, sunlight, electromagnetic radiation, and a reasonable amount of force, and it must be reliable even after being subjected to water and a variety of solvents. Thus, the issue of alternate communication/power transfer technologies is closely associated with the type of encapsulating materials and the tag fabrication, and each technology was evaluated for its impact on these issues.

Finally, an evaluation was made for each of the technologies concerning the specific applications to a SDT system. In particular, the size and cost requirements were compared in a relative fashion to each other, as well as those the alternative technology should not require that the data carrier be substantially larger than the "dog tag"-sized unit presently considered, and the total tag cost cannot be greater than the expected financial returns.

After each design was carefully assessed, the seven technologies were rank ordered from most to least promising. Table 4.11 contains a summary matrix of the technology assessment. A complete description and evaluation of the technologies is presented below. Each discussion is preceded by a brief overview or abstract of the concept; however, if more information is desired, the reader is invited to review the detailed description and assessment.

Inductive Coupling. From past experience on similar projects, the Battelle team has found that inductive coupling holds considerable promise for establishing the communication/power transfer interface between a system data tag interface device and a portable data carrier. Therefore, it is not surprising that the inductive coupling concept is the primary technology recommended for further consideration in a SDT system. The concept relies on the magnetic coupling between a pair of coils, one just under the surface of a Soldier Data Tag, and one as part of the Soldier Data Tag system reading element. After the mating coils are brought into close proximity to each other the coupling is established, and two-way communication can take place. Furthermore, power can be transmitted across the medium and transformed into a form usable by the tag circuitry. Therefore, no battery is required to power the embedded memory, computer, and associated communication hardware.

The concept appears highly suited for application to the SDT system and the associated environment. The sealed tag is impervious to contaminants, the inductive coupling is virtually unaffected by the conditions presented above. The concept's reliability is quite high, and the technology is well understood. In fact, similar concepts have been used in a variety of applications outside of the portable data carrier arena. Lastly, the hardware costs for the interface along (not including reader to tag circuitry) are trivial.

TABLE 4.11. TECHNOLOGY ASSESSMENT MATRIX

Technology	Relative Tag Cost (1 = low, 10 = high)		Relative Tag Interface Device Cost (1 = low, 10 = high)		Relative Size (1 = small, 10 = large)		Maintainability	Advantages	Disadvantages	Rank Order (1 = lowest, 10 = highest)
	1	4	6	9	1	3				
Direct Contact	1		1		1		Contacts may need cleaned.	Simple, small tag, low cost.	Contacts wear out; vulnerable to environment.	6
Inductive Coupling	4		5		3		Little or no maintenance.	Powered by reader; tag totally sealed and protected.	Circuitry more complex than direct contact.	9
Radio Frequency Waves	6		10		7		Little or no maintenance.	Tag totally sealed; read tag from a distance.	Requires high power, tag size large.	7
Electromagnetic Waves	9		10		10		Requires battery replacement.	Tag totally sealed; read tag from a distance.	Needs imbedded power source; tag size impractically large.	1
Magnetic Hall Effect	6		7		5		May require battery replacement.	Tag totally sealed; simple communication.	Needs imbedded power source; requires considerable development.	3
Optional Coupling	3		4		2		Periodic cleaning. May require battery replacement.	Tag totally sealed; simple communication not affected by EM radiation.	Requires good optical path; needs imbedded power source.	8
Acoustic/	5		5		4		May require battery replacement.	Tag totally sealed; requires little power.	Needs imbedded power source; requires considerable development.	2

Coils can be inexpensively wound on spools in a solenoid geometry or etched on a printed circuit board in a planar arrangement.

Although the power coupling and communication systems are not typically combined into a single pair of coils, the system is potentially quite reliable. Signal isolation is a common function of transformers, and air core transformers are particularly adapted to this use since they are not frequency limited by hysteresis and other core losses. Some implanted heart pacemakers have successfully used inductive coupling to recharge the unit's batteries. In addition, frequency shift keying has been commonly employed for transmitting digital information over other alternating current media such as radio waves and microwaves.

Once the tags are fabricated with the induction coil, the reader is retrofitted with a mating coil, the system is easily maintained, requiring little or no further human interface. Power comes from the reader, so no batteries need to be replaced. The tag is completely sealed, and the benefits of the encapsulating material can be maximized. Furthermore, the tags are tamper-proof and can be constructed to have no distinguishable or identifiable features or markings, adding a small element of security to the tag. The material will cover the entire embedded circuit without the need to bring connections to the surface or to make other aberrations in the protective surface.

Although close proximity is required to maximize the efficiency of the coupling, the system is technically considered noncontact. A layer of air or any diamagnetic and nonconducting material, such as wood, plastic, or oil can be inserted between the coils without any degradation in system performance. Thus, the only additional requirement placed on the protective material is that it is to be diamagnetic and not influence the magnetic field. Most polymers, by their very nature, have this characteristic.

In many respects the inductive coupling technology appears well suited for the Soldier Data Tag application. System performance is not compromised by water, fuel, solvents, sunlight, or temperature, and most of the limitations are defined by the circuitry. The small size of the tag can be realized, and the additional component cost required to realize noncontact data communication can be kept quite low, probably on the order of \$15 to \$20 per tag.

Optical Coupling. The second most appropriate technology, the concept of optical coupling, allows communication between a SDT system and microcomputer embedded within a data tag via an optical path. Two optically isolated pairs, each having a transmitting and receiving element, allow for communication in both directions. Therefore, the SDT tag interface device and the embedded circuit in the tag each provide half of each optical isolator. By properly interrupting the light beam between the elements, digital data can be directly transmitted across the optical medium, so interface circuitry and data decoding can be quite simple. However, the concept does not provide its own power like the inductive coupling technology, so a separate power source, such as implanted battery, must be applied.

The technology appears suitable for applications to SDT system provided the optical components are well protected from the harsh environmental elements. (It should be noted that an optical technology must be protected from the environment in order to insure the integrity of the optical data path. Methods of accomplishing this include the use of protective "hatch" covers which are removed during the communication process.) Optical isolation is quite reliable and frequently used in digital equipment interfaces. It is virtually immune to electrical noise and can handle exceedingly high data rates. Furthermore, the optical elements can be easily integrated into the microcircuitry so that both size and cost are kept small.

After careful evaluation, the optically isolated coupling appears to have merit for this application. Its reliability is apparently quite high; optical isolation is frequently used in computer input/output gear, primarily because of its low susceptibility to electrical noise and the fast data rates that can be achieved.

Except for periodic inspections and occasional cleaning of the optical "windows" if incorporated into the design, the data coating unit requires little maintenance. The tag is a sealed unit and impervious to most environmental factors. If batteries are used, periodic maintenance is required, but the circuitry can be designed to extend battery life by allowing power activation only upon receipt of an initial input signal. After data transmission has occurred and is no longer in progress, battery power would be shut off after some prescribed time. Thus, the useful life is lengthened and the frequency of battery maintenance is minimized. In general, though, the

Battelle team recommends against the use of batteries. The volume of data tags translates into large maintenance and battery costs, particularly if batteries are replaced periodically to maintain consistent operation. An alternative is to monitor battery voltage as it discharges, but without electrical contact, battery checking systems are difficult to implement.

Strictly speaking, the interface is noncontact, although this design requires close proximity and proper alignment of the tag interface device to the data tag to ensure the proper operation of the system, unlike the wide spatial tolerances allowable in the inductive coupling system. Normally, an optical system such as this could not tolerate a harsh environment, but the design has an added measure of protection since the protective material completely encloses the embedded component and yet allows light to propagate through it. In addition, the optical components are not susceptible to electrical noise created by electromagnetic radiation.

Finally, the design is applicable to TC/M systems in both size and cost. The added components are small enough to be easily incorporated into a dog-tag sized data carrier with the present microcomputer and memory, and the total component cost per tag can be kept down to approximately \$10 to \$15.

Radio Frequency. The primary advantage of the radio frequency coupling concept is the ability to communicate with soldier data tags from a distance. However, several provisions must be made to achieve this capability. First, the reader transmitted power must be increased as the distance between the reader and tag antennas increases. In fact, received power is a function of the inverse distance squared for a linear antenna. That is, to receive the same amount of power after the distance is doubled, the transmitter power must be increased four-fold. One way to reduce the power transmission loss is to use a directional antenna that focuses the emitted energy into a beam. Parabolic or dish antennas perform such a function.

As distance is increased, the potential for distortion and cross-talk from adjacent data tags is increased. One provision is to use a wide bandwidth system and a tunable reader. Each soldier data tag would communicate on its own set of frequencies. Unfortunately, the bandwidth of frequencies would quickly be exhausted, and system could not support several tags each having its own frequencies. And, the amount of effort to tune to each

unknown carrier frequency of the data carriers would be laborious indeed, even if performed electronically and automatically. An alternative is, again, to use a directional antenna and a single set of frequencies. With the communication link focused on one particular tag, the signal-to-noise ratio is increased to reduce interference and the impact of stray fields from other tags. Of course, the antenna and tag location are still critical to proper operation, because more than one tag cannot be within the effective path of the reader antenna without significant distortion.

Radio frequency coupled systems are apparently reliable and have been used quite successfully in industrial environments. The tool fault detector is a battery-powered, radio frequency transmitter coupled to a clutch in a machine tool holder. Normally, the transmitter is mute, but when a tool binds, the clutch disengages and the transmitter emits a constant tone signal. Housed within the tool holder assembly, the device can transmit a signal to trigger a monitoring receiver several feet away.

A more sophisticated device is sold by Indentronix, Inc., and is used as an identifying tag on inventory items, railroad cars, products on an assembly line, and even cattle. The identification module is approximately the size of a cigarette pack and contains a preprogrammed signature. When a radio frequency signal from a monitor strikes a module, a certain amount of energy is imparted to the internal circuitry. The module echoes its unique signature to the monitor, which specifically identifies that particular item. Although interactive communication does not take place, bidirectional transmission does occur.

Generally speaking, rf-based systems are well adapted to a variety of environments. They are virtually unaffected by surface contaminants and can even be read from a distance. The absence of batteries allows the modules to be easily maintained. Because of its similarities to the inductive coupling concept, many of the same arguments can be made for the radio frequency coupling concept.

The issues of applicability to SDT systems must still be resolved. The cost and need for such a system must be carefully examined, and the economic advantages (if any) of having read-from-a-distance capability must be carefully weighted. If reading from a distance is not important, it is probably more prudent to adopt an inductively coupled system rather than an

rf-based system. Secondly, this capability might provide an easily observed "signature" to the enemy in wartime. The physical size of the module must still be determined, which is largely a function of the communication distance that must be defined. For example, one of the reasons why the Indentronix module is so large is because the distance of transmission, particularly during high speed (e.g., moving railroad cars), necessitates a rather large antenna at the module. In most cases, the antenna size dictates the data carrier size. Finally, the efficiency and suitability of a directional reader antenna and multiple tags must be completely assessed.

Electromagnetic Waves. Idealistically, the above three technologies all involve electromagnetic (EM) waves of one form or another. However, this concept is concerned with EM waves of frequencies greater than radio waves and less than optical waves. One example would be microwaves, such as those used in the system marketed by Philips called PREMID (Programmable REMote IDentification). Basically, all of the arguments for a radio link apply equally well except for two major drawbacks concerning its application to Soldier Data Tag systems.

First, most of the present microwave systems require a battery. Although a different power source could be employed, such as induction or photovoltaic cells, these require close proximity of the reader to the tag, thus eliminating the read-from-a-distance characteristic. The second disadvantage is the tag size, generally about five to seven inches long and two inches on a side. Much of this space is reserved to house long-life batteries, but the biggest constraint is the antenna size. Many of the microwave and other electromagnetic wave systems require relatively long antennas and are difficult to scale down to a size suitable for the Soldier Data Tag system. Thus, in general, these physical limitations precluded electromagnetic wave systems from further consideration for SDT systems.

Magnetic Hall Effect. Similar to the optical coupling scheme, which uses a photodiode/phototransistor pair, the concept of magnetic hall effect uses a coupled magnetic field source and a hall effect sensor. The magnetic field source could be as simple as an electromagnetic, whose field strength increases with increasing coil current. A hall effect sensor is a device that

responds to the field with an output voltage linearly proportional to the field strength, up to saturation. Like the optical coupling, this concept requires a separate power source at the embedded circuit module. The technology is not recommended for SDT application because considerable development would be required to adapt the concept.

Acoustic/Piezoelectric. This concept, too, is similar to the optical coupling. Here a pair of piezoelectric resonators, one at the SDT reader and one at the data carrier, operate as acoustic microphones and speakers. To transmit data to the tag, electrical energy is applied to the reader resonator to make it act like a speaker, an acoustic energy source. The acoustic waves are received by the tag resonator, acting like a microphone, and converted into an electrical signal. To transmit information in the opposite direction, the roles of piezoelectric resonators are reversed. Again, like the optical coupling, the concept is not self-powered, and a separate data tag power source is necessary. The primary drawback prohibiting this technology's application to SDT systems is, again, its largely conceptual nature, requiring considerable development effort to bring the technology to maturity.

4.3.3 Tag Interface Device Design Issue Summary

The nature of the TID functions make its design both critical and difficult. In particular, the host interface and data manipulation functions will be driven by all applications of the SDT system, either in its original fielding or added later. Difficulties in making changes once the system has been fielded put extra emphasis on the need for flexibility, and on the importance of rigorous design review prior to implementation.

Specific hardware design issues, notably the tag interface and host interface, may be more significant economically and have a more global impact than currently thought. Firmware design is an issue which has received little attention to date but is capable of dominating the success of the system. Requirements for this function come more from interactions with host ADP systems than from the rest of the SDT system, and thus are not under control of the SDT system designers. Regarding security, the TID in general and its

firmware in particular are likely points of attack. Design tradeoffs between software configurability and security may force an increase in TID complexity.

4.4 Conclusions

Based on the previous discussions regarding the physical design of the SDT system, several conclusions can be reached. First, regarding the information storage technology for the SDT, both electrically erasable memory (EEPROM) and the optical stripe appear to have attributes which satisfy the basic requirement for the tag. However, the survivability of an optical stripe in the envisioned battlefield environment is uncertain. The EEPROM has a longer track record, and has demonstrated survivability success in the prior Army experiments. If a rapid fielding of the soldier data tag system is to be accomplished, then the most logical choice is the use of the EEPROM/processing structure based on the prototype systems. It should be noted, however, that the current system still needs rigorous testing and design revisions in order to result in a design which meets the Army's overall requirements now and in the future.

From the information previously presented in the materials section, it can be concluded that a polymeric encasement is the most probable approach to an effectively operational SDT. Through understanding the critical importance of the survivability of the SDT in tactical situations, it can be concluded that the mechanical properties are the least important requirements to be met, with the most important requirements being physical, electrical, and chemical properties. These requirements can most probably be met by two of the candidate materials: liquid crystal polymer (LCP) and polyphenylene sulfide (PPS). therefore, they should be considered as viable polymers for the SDT application.

Based on the materials and processing cost/benefit analysis, it is expected that the equipment life will be diminished by at least half, and utility costs will double with the use of PPS. As a result of the estimate of materials, utilities, and labor costs, the total unit cost for the SDT made from PPS is only 4 cents/unit more than compared with the costs of a SDT made from LCP. However, a greater savings may be realized by the use of LCP if equipment life and costs are taken into account.

Finally, in a tactical situation the SDT would be an improbable source for detection by any of the following methods: IR photography, chemical, sound, electronic, radar or reflectance. In addition, there are several viable printing techniques which can be used in the field to apply surface information to the SDT. These printing methods could include either a reverse coating or electrophotographically imaging the required information on a film then laminating it to the SDT. Such applications are fast and relatively simple; the equipment should be quite mobile; and the lamination will provide mechanical and chemical protection for the surface information.

It is our opinion the concept of the SDT is feasible from a materials viewpoint for both wartime and peace situations, and in most cases the polymeric encasement will probably outlive the usefulness of microchip.

Finally, the discussion in this section has also addressed some preliminary issues regarding the tag interface device section of the system. From the Army documentation received thus far by Battelle, it appears that this aspect of the system has seen the least amount of design development. Several reader concepts exist, however, the manner in which these are to be connected to other systems, and the nature of applications software which resides in the tag interface device still needs a thorough design phase. Some of the issues which will impact this design are discussed in Chapter 6, "ADP System Compatibility".

4.5 Recommendations for Component Level Design Issues

Based on the analysis presented in this section, the following recommendations are provided:

- Plan to build tags of LCP impregnated with fillers to provide shielding, EEPROM, and metallic contacts.
- Study materials alternatives to provide the best corrosion resistance for the metallic contacts.
- Use an interface protocol with the tag which would allow future expansion of storage capacity and hardware security provisions.

- Study the demands made on the design of the TID by the variety of anticipated applications.
- Study the specific instances where the SDT development efforts can be integrated with ADP host system development in order to reduce the instances of duplicate development efforts.

GLOSSARY OF POLYMER/PROCESSING TERMINOLOGY

Amorphous - Non-crystalline structure. The distribution of polymer chains in the matrix is completely random.

Coefficient of linear thermal expansion - The fractional change in length of a material for a unit change in temperature.

Continuous service temperature - The highest temperature at which a material can perform reliably in a long term application.

Dielectric strength - The voltage that an insulating material can withstand before dielectric breakdown occurs.

Flash - Extraneous polymeric material that escapes from the mold, either at the mold parting line or a vent, which remains attached to the molded part until removed by machining.

Heat deflection temperature (HDT) - The measure of temperature at which a specimen deflects 0.01 inch under a specific load.

Izod, notched - The energy required to break a specimen in which there is a V-notch to create an initial stress point.

Melt flow - Rate of extrusion of molten resin through a die of a specified length and diameter.

Melt temperature - The temperature at which a polymer obtains sufficient thermal energy to enable its chains to move freely enough for it to behave like a viscous liquid.

Melt viscosity - Viscosity of a polymer when it is the molten state.

Mold shrinkage - The difference between the size of the part and the size of the mold cavity.

Surface resistivity - The ratio of the potential gradient parallel to the current along its surface to the current per unit width of the surface.

Tensile strength, break - The maximum stress that a material can withstand without breaking when subjected to a stretching load.

Thermoplastic - A material which is adequately rigid at normal temperatures and under normal stress conditions but is capable of deformation under heat and pressure.

Thermoset - A material which will undergo or has undergone a chemical reaction by the action of heat, catalysts, ultraviolet light, etc., leading to a relatively infusible state.

Vicat softening point - The temperature at which a flat ended needle will penetrate a specimen under a specified load using a uniform rate of temperature rise.

Volume resistivity - The reciprocal of conductivity, measured by the resistance of a body of unit cross-section and of unit length at 0°C.

Water absorption, 24 hours - The percentage of water absorbed by a material when immersed in water for 24 hours. Water absorbed in a material chiefly affects its electrical properties.

5.0 COST/BENEFIT ANALYSIS

The objective of the cost benefit analysis was to determine what factors most strongly affect costs and benefits of SDT systems. In particular, the study concentrated on factors previously determined to be important: tag capacity, hardening, security, and areas of application.

The approach for the CBA was to build a model of costs and benefits for SDT systems, then examine several sets of assumptions using the model. In choosing these sets of assumptions, the project team attempted to span the range of possibilities, rather than to determine the exact specifications. Undoubtedly, as the actual SDT system specification is developed it may differ from any of these sets of assumptions. The intent of this study is to provide the model with which the actual specification can be evaluated, and to provide information to assist in the system design. Numbers and applications for SDT systems given in this analysis are to be regarded as test cases only; specific conclusions are itemized at the end of this section. The remaining section is divided into the following subsections:

- **5.0.1 Introduction to the Cost/Benefit Analysis.**
- **5.0.2 Scope of Cost/Benefit Analysis.**
- **5.1 Analysis Approach.** A discussion of the scope, assumptions, and methods used for the analysis.
- **5.2 Results of the Peacetime Cost/Benefit Analysis.** Presenting the wartime and peacetime cost and benefits.
- **5.3 Conclusions.** Providing insights and recommendations based upon the CBA.

The appendix shows the details of the cost/benefit analysis methodology.

5.0.1 Introduction to the Cost/Benefit Analysis

A study of cost justification is required to determine which applications of the SDT system should be implemented first. Cost justification exists when the benefits of a system outweigh the burdens of the system. Examples of cost justification include:

- The system causes the war to be won at an acceptable cost
- The system provides a current function more efficiently and, therefore, provides more benefit at some cost saving over the older system.

SDT primarily falls into the second category of cost justification by potentially providing a current service more efficiently. Transactions will be performed more efficiently and correctly using SDT to queue automated files and will allow files to be available where they have never been available before (e.g., when on travel away from home station - TDY). The cost/benefit analysis was performed to determine if the increased efficiency was cost effective. SDT's role during the wartime scenario was also investigated at this time in a more qualitative manner.

Three general SDT concepts are included in this study. These systems differed in memory capacity, hardening, security, and cost. The results of the cost/benefit analysis were combined with the security, interfacing, and materials results to determine which concept should be developed.

5.0.2 Scope of Cost/Benefit Analysis

The original scope of the CBA was to study both wartime and peacetime applications of the SDT. In the peacetime scenario, a model based on quantitative data was developed. In wartime, a qualitative analysis was more appropriate.

Cost and benefits for the Army (active, reserve, and guard) in the areas of personnel, finance, and medical were considered for the analysis. The analyses considered the costs and benefits as differences from the current methods of achieving personnel, finance, and medical applications for the entire Army. That is, since SDT's primary function is to enhance current capabilities only the differences from the current capability were considered. Examples of this include the cost of procuring the tags (an added cost to current techniques), and the benefit of personnel time savings during interactions (a benefit over the current techniques).

The three SDT concepts analyzed range from a low capacity system to a high capacity system. SDT1, the designation used in this report for the

"minimum" tag, is a 2K-bit chip, inexpensively processed (e.g., no hardening), with low security requirements, a low unit cost, and a low number of access points. SDT1 would be used for identification and calling up computer files. SDT2, the current prototype tag, is the "median" tag consisting of a 64K-bit chip, medium process complexity (e.g., some hardening), medium security, medium unit cost, and medium number of access points. SDT2 would be used as SDT1 and would also contain a great deal of immediately available data. SDT3 is the "maximum" tag consisting of a 256K-bit chip, high security, complex processing (e.g., hardened), and a large number of access points. The use of SDT3 would be similar to SDT2 but would allow for expansion to other types of information that may not fit on a 64K chip. **The additional data storage in SDT3 would allow an expanded information file, permitting more detailed and longer historical records.**

5.0.3 Data Collection

Documents on SDT concept demonstrations and analyses provided by the Army (listed in the bibliography) were reviewed and provided some data for the CBA. Battelle experts in software, materials, and security were interviewed to determine impacts of their concerns on SDT concepts, costs, and benefits. Most of the data collected and used in the CBA came from Army experts in the fields of personnel, medical, finance, reserves, and SDT. Many of the persons interviewed had experience in the SDT demonstrations as well as an area of application. They were the sources of time estimates for transactions.

The interviews were accomplished using a questionnaire developed by Battelle for the Cost/Benefit Analysis task. The questionnaire structured the questioning but also allowed flexibility. The questionnaire consisted of five pages of questions. Two Battelle employees were responsible for the data collection. One person asked the questions and both persons recorded the answers for comparison and clarification.

The SDT Program Office was another major source of data, providing equipment unit costs, research and development costs for hardware, production schedules, and some transactions data. The SDT Program Office also aided the analysis by identifying Army experts and arranging interviews for Battelle.

Telephone interviews were used to fill any data holes that remained after the personal interviews at Ft. Benjamin Harrison. Telephone interviews were also used to update data as the SDT budget status changed during the program. The analysis described in this report is based upon the budget information available March 18, 1985, the date of the last analysis update.

5.1 Analysis Approach

5.1.1 Evaluation Criteria

There were two evaluation criteria used in the cost/benefit analysis. One criterion was a measure of peacetime cost/benefits and the other is a measure of wartime benefits. The peacetime measure of effectiveness is the dollar difference between today's system without the SDT and today's system with SDT. The wartime measure of effectiveness is the difference in personnel availability for a European war on day 30 between today's Army and today's Army with SDT.

Today's Army (with automation) was used as the baseline for both peacetime and wartime evaluation in order to measure SDT's contribution to the "Army of Excellence" plan in the area of personnel freed from administrative positions for use in combat positions.

Two measures of effectiveness were used, since it was designed to see peacetime and wartime results separately. Most of the conclusions derived from the CBA are based on the peacetime results only because insufficient data were available for the wartime scenario resulting in a qualitative discussion of wartime benefits.

5.1.2 Assumptions

Several assumptions had to be made in order to compute consistent values that were comparable between the SDT concepts. The assumptions were kept to a minimum and may be changed as the SDT program progresses.

Costs and benefits of the SDT were computed as the difference (deltas) between today's Army with automation but without SDT and today's Army with automation and with SDT. The non-SDT automation included the Unit-Level

Computer (ULC). The differences were computed for the personnel in today's Army, including active, reserve, and guard components. Today's Army was chosen as the baseline in order to determine SDT's role in achieving the Army of Excellence by freeing up administrative personnel.

A 10-year life was assumed for both the tags and the tag interface devices. A 10 percent annual failure rate, also assumed, is based on the 10-year life assumptions. Army estimates of expected life is 10 years for the tags and associated hardware. Assuming that all items are throwaway, the failures would be distributed around the 10 years (e.g., for a normal curve, 10 years would be the average life). However, since no failure data were available for the three general SDT concepts or for their associated hardware, it was assumed that all items would be replaced once during the expected life. That is, one tenth of the items would be replaced per year for 10 years. Such an assumption is pessimistic since 100 percent of the items will be replaced in 10 years versus the 50 percent that would be replaced if failures were normally distributed. As more data become available with the development of SDT, corrected failure rates should be used. Also, inherent in the 10 percent failure rate is the assumption that all SDT equipment is throwaway. Repair may reduce the operation and support burden and should be investigated.

An 18 percent annual turnover of Army personnel and a 5 percent annual loss of tags were assumed. Eighteen percent turnover coincides with the Army Force Planning Cost Handbook (1983) turnover rate. A 5 percent annual loss is assumed based upon losses to the limited number of tags in the field and upon dog tag history of losses.

Fielding was assumed to start in FY 87 based upon the projected SDT production schedule dated March 8, 1985. Costs/benefits of tags is dependent upon the production schedule. Therefore, the analyses were updated several times during the project in order to record costs/benefits accurately.

Cost/benefits of planned automated systems were not included in the CBA. It was assumed that these systems will be in existence when SDT is fielded. The cost/benefit "deltas" computed in this study reflect only SDT cost/benefits, not automated systems. An example of an automated system benefit not included is the paper savings and associated storage deleted due to automating the files. These are not attributable to the SDT system; two savings came as a result of other ADP systems.

Personnel levels for the time saved or added due to SDT varied significantly. An E-6 was assumed as the average pay and allowance grade. An E-6 is probably high for clerk time but is, at the same time, probably low for administrative and supervision time. E-6 is believed representative of the average grade.

5.1.3 Analysis Methodology

The costs and benefits of the SDT fall into two general categories: tangibles and intangibles.

Tangible cost/benefits are those costs and benefits that can be represented by a dollar value, such as the value of personnel time saved or lost. Intangible costs and benefits are those costs and benefits that cannot be represented by a dollar value, such as return-to-duty rates during a war. The value of an increased return-to-duty rate on battlefield effectiveness far outweighs the dollars that might also be saved.

Figure 5.1 shows the matrix used to compute the tangible costs/benefits. The costs/benefits are broken out by application for each SDT concept. The matrix is a modification of the matrix used in Army Pamphlets 11-2 through 11-5. R&D (Research and Development) and Investment costs are primarily costs due to SDT. They are the cost of developing, procuring, and initializing the use of SDT. O&S (Operations and Support) are the additional annual costs or annual benefits due to SDT. O&S is the area where peacetime cost savings may occur by upgrading the current system with SDT.

Each cost and benefit of SDT was computed as a delta from the current system. That is, under O&S, facilities entries reflect the cost to maintain the additional or saved facility space due to the use of SDT.

The reader should note that the tangible cost/benefits are peacetime only cost/benefits. Results listed in a tangible matrix would show how much extra, or savings, occurs due to SDT during peacetime operations.

Appendix 1 shows the details of the tangible computations. Each "cost" category is numbered using Army Pamphlet 11-5 notation and defined in Appendix 1. The line numbers are shown in Figure 5.1 and correspond to the cell numbers listed on the divider sheets in Appendix 1. Therefore, to find the computation method for O&S equipment one should go to the divider titled

SDT CONCEPTS CATEGORY	1				2				3			
	COMMON	MEDICAL	PERSONNEL	FINANCIAL	COMMON	MEDICAL	PERSONNEL	FINANCIAL	COMMON	MEDICAL	PERSONNEL	FINANCIAL
1.0 RAD COST												
1.1 HARDWARE	1,900	---	---	---	1,900	---	---	---	1,900	---	---	---
1.2 SOFTWARE	---	100	100	100	---	375	375	375	---	375	375	375
2.0 INVESTMENT COSTS												
2.1 TAGS	5,213	---	---	---	52,126	---	---	---	369,722	---	---	---
2.2 EQUIPMENT	---	4,139	1,340	520	---	8,275	2,688	1,038	---	8,275	2,688	1,038
2.3 TRAINING (IN-SITE ACTIVATED)	---	---	---	---	---	---	---	---	---	---	---	---
2.4 TECH DATA	15	---	---	---	48	---	---	---	600	---	---	---
2.5 SITE ACTIVATE	---	16,795	814	533	---	25,064	819	533	---	25,064	819	533
2.6 INITIAL SPARES	---	---	---	---	---	---	---	---	---	---	---	---
2.6.1 TAGS	1,616	---	---	---	16,159	---	---	---	68,696	---	---	---
2.6.2 EQUIPMENT	---	414	134	52	---	828	269	104	---	628	269	104
3.0 OPERATIONS AND SUPPORT												
3.1 FACILITIES	---	---	---	---	---	---	---	---	---	---	---	---
3.2 PERSONNEL	---	---	---	---	---	---	---	---	---	---	---	---
3.2.1 TRANSACTIONS	---	-360,058	-38,038	?	---	-360,058	-923,099	?	---	-360,058	-923,099	---
3.2.2 MANIFESTS	---	---	-1,629	---	---	---	-1,629	---	---	---	-1,629	---
3.3 TRAINING	---	-7,201	-761	?	---	-7,201	-18,462	?	---	-7,201	-18,462	?
3.4 SPARES/SUPPLIES (TAGS)	13,215	---	---	---	132,146	---	---	---	584,723	---	---	---
3.5 SECURITY	---	-55,200	---	?	---	-55,200	---	?	---	-55,200	---	?
3.6 MASTERFILE	---	---	---	---	---	---	---	---	---	---	---	---
3.7 EQUIPMENT	---	4,139	1,236	448	---	7,613	2,473	955	---	7,613	2,473	955
3.8 SOFTWARE	---	184	184	184	---	690	690	690	---	690	690	690
4.0 COLUMN TOTALS	21,958	-396,688	-36,620	?	202,378	-379,614	-935,876	?	1,025,642	-379,614	-935,876	?
5.0 CONCEPT TOTALS												
		-409,513				-1,109,417				-286,153		

FIGURE 5.1. DOLLAR COST AND BENEFITS OUTPUT MATRIX

"Cell Number 3.7, Equipment". The computation method is listed and described on a "Cost Data Sheet", shown in Figure 5.2, which is based on the Army Pamphlet 11-5, "Cost Data Sheet".

The calculation, data, and data sources are found on "Data/Computation Sheets" that follow directly behind their corresponding "Cost Data Sheet". (See Figures 5.3 through 5.5.) Each data sheet corresponds to one or more columns of the matrix shown in Figure 5.1. For O&S equipment, all medical computations are found on one sheet. The sheet is labeled "Cell No. 3.7, M" (Figure 5.3). Calculations are given for SDT1, 2, and 3 on the one sheet. Figure 5.4, labeled "Cell No. 3.7, P", shows the calculations for personnel equipment, and Figure 5.5 shows the calculations for finance (F) equipment.

Table 5.1 lists the intangible costs and benefits analyzed. Very little data were available for intangibles. Conflicting views of roles for the SDT in premobilization/mobilization were given by the persons interviewed. Battalion airlift manifesting can be achieved in one hour using SDT versus 49 hours, but the SDT's role in POR (Processing for Overseas Replacement) was debated. Some combat personnel stated that the battalions scheduled to mobilize in the event of war are in a ready status. That is, medical, financial, and personnel requirements for mobilization have been met and are updated as necessary to stay in an alert status. Having SDT, they argue, will

TABLE 5.1. INTANGIBLE COSTS/BENEFITS

-
-
- Battlefield Effectiveness
 - Premobilization/mobilization and deployment
 - Lives saved
 - Personnel availability
 - Return to duty date
 - Replacement operations
 - Average Processing Time
-
-

Cell No.: 3.7Date: 3/6/85Cost Data Sheet

Item: Equipment

Cost Data Expression:

$$EQ = F_t \times F1 \times C_E$$

Included:

Excluded:

Variables:

 F_t = Time factor - in equivalent years $F1$ = Failure rate of equipment C_e = Equipment investment cost, Cell number 2.2

FIGURE 5.2. COST DATA SHEET FOR O&S EQUIPMENT

Cell No. 3.7, MPage No. 1Data/Computation Sheet

Data:

<u>Variable</u>	<u>Value(s)</u>	<u>Source(s)</u>
F _t	9.2	Computed, see Cell number 3.2.1, Medical, P2
F _l	10%/yr	Assuming 100% turnover in 10 years
C _E , SDT1	\$4,030,500	Computed, see Cell number 2.2
SDT2, 3	\$8,060,800	

Computation:

$$\begin{aligned} \text{EQ for SDT1} &= 9.2 \times 1 \times 4,030,500 \\ &= \$3,708,060 \end{aligned}$$

$$\begin{aligned} \text{EQ for SDT2 or 3} &= 9.2 \times 1 \times 8,060,800 \\ &= \$7,415,936 \end{aligned}$$

FIGURE 5.3. MEDICAL DATA/COMPUTATION SHEET FOR O&S EQUIPMENT

Cell No. 3.7, PPage No. 1Data/Computation Sheet

Data:

<u>Variable</u>	<u>Value(s)</u>	<u>Source(s)</u>
F_t	9.2	Computed, see Cell number 3.2.1, Medical, P2
F_1	10%/yr	Assuming 100% turnover in 10 years
C_E , SDT1	\$134,400	Computed, see Cell number 2.2
SDT2, 3	\$268,800	

Computation:

$$\begin{aligned} \text{EQ for SDT1} &= 9.2 \times 134,400 \times 1 \\ &= \$123,648 \end{aligned}$$

$$\begin{aligned} \text{EQ for SDT2 or 3} &= 9.2 \times 1 \times 268,800 \\ &= \$247,296 \end{aligned}$$

FIGURE 5.4. PERSONNEL DATA/COMPUTATION SHEET FOR O&S EQUIPMENT

Cell No. 3.7, FPage No. 1Data/Computation Sheet

Data:

<u>Variable</u>	<u>Value(s)</u>	<u>Source(s)</u>
F_t	9.2	Computed, see Cell number 3.2.1, Medical, P2
F_1	10%/yr	Assuming 100% turnover in 10 years
C_E , SDT1	\$485,300	Computed, see Cell number 2.2
SDT2, 3	\$970,600	

Computation:

$$\begin{aligned} \text{EQ for SDT1} &= 9.2 \times 1 \times 485,300 \\ &= \$446,476 \end{aligned}$$

$$\begin{aligned} \text{EQ for SDT2 or 3} &= 9.2 \times 1 \times 970,600 \\ &= \$892,952 \end{aligned}$$

FIGURE 5.5. FINANCE DATA/COMPUTATION SHEET FOR O&S EQUIPMENT

not speed up the process. Also, combat personnel felt that aircraft will not be available for mass mobilization, which would allow additional time for POR. SDT may play a role in the second and third waves of mobilization, and also in pre-mobilization, where shot records and the like could be scheduled on the SDT. Scheduling requirements with SDT will help maintain a ready status for mobilization.

Lives saved or lost due to SDT during wartime was not obtained. Interviewees were asked the percentage of lives that may be saved if emergency data were available on the battlefield. Estimates ranged from 10 percent to 50 percent.

Personnel availability refers to the people added or deleted from administrative jobs due to SDT. Soldiers time added or deleted was not used in the computation of administration savings, but was used as a benefit elsewhere. In medical, the number of administrative person-years saved per year equals:

$$\frac{8,811,615 \text{ transactions/yr} \times 14 \text{ min/transaction}}{60 \text{ min/hr} \times 2000 \text{ hrs/yr}} =$$

1000 man-years/yr (see Cell No. 3.2.1, M in Appendix 1)

Personnel savings calculations for personnel application were computed in a similar fashion and are shown in Appendix 1, Cell No. 3.2.1, P. No financial savings of personnel were identified.

No data were available on return-to-duty rates or on replacement rates. SDT tests completed to date have not evaluated SDT for this measure of merit and, like lives saved, was a very controversial subject with the interviewees. Estimates ranged the total gamut from no improvement to 50 percent improvement.

Average processing time saved or added is:

14 minutes for emergency medical (see Cell No. 3.2.1, M--
14 minutes saved per person)

The time savings are shown for personnel applications in Table 5.2 by type of transaction. Weighted time savings were computed using the annual rate as the weighting factor. The equation is:

$$\frac{\sum_{\text{Transaction Types}} \text{Annual rate} \times \text{Time saved/added}}{\sum_{\text{Transaction Types}} \text{Annual rate}}$$

Battlefield effectiveness was not computed due to lack of data at the present time. However, there appears to be a battlefield benefit arising just from the increase of personnel available for combat. An analysis of the sensitivity of battlefield effectiveness to the use of SDT was performed as part of the CBA. Personnel availabilities were assumed with different SDT effects. The results of personnel availability on day 30 were compared to test sensitivity of battlefield effectiveness. The sensitivity computations and results are shown under "Results".

TABLE 5.2. PERSONNEL APPLICATION, PERSONNEL TIME SAVINGS

Transaction Type	Annual Rate/Soldier		Time Saves (-)/Added (+) (hours)	
	SDT1	SDT2/3	SDT1	SDT2
In Process	0.4	0.4	-14.4	-144
Out Process	0.4	0.4	-14.4	-144
File Update	0.2	11.2	-72	-72
Tag Update	--	3.5	--	+0.03
Initiate File	--	0.18	--	--
Reconstruct File	--	0.05	--	-1,392
Errors	0.254	0.254	-96	-96

Average (SDT1) = 40.1 hours/transaction.

Average (SDT2/3) = 63.5 hours/transaction.

5.1.4 Results of Wartime Benefit Analysis

SDT is currently in concept formulation, a time during which very little quantitative data are available. SDT has had some testing, which allows for some data. However, the results of the test are more qualitative than quantitative. Peacetime data were available to some extent but wartime data, at this point, is lacking.

Battlefield effectiveness is a measure of merit defined as the availability of personnel on the battlefield. Battlefield effectiveness is a combination of replacement rates, return-to-duty rates, and casualty rates. SDT has been identified as a means of identifying needed MOS's in a more timely manner and therefore increasing the probability of getting a correct placement in less time. SDT will carry medical records into battle allowing rapid medical checks in emergency. The emergency data are expected to save lives and, with quicker correct treatment, increase the return-to-duty rate. How much improvement is indeterminable at the time of this study.

Estimates of improvements in troop availability in wartime were based on an assumption of 95 percent for the baseline availability. This can also be viewed as a 5 percent loss per day. If the SDT system can reduce this loss to 4.5 percent per day (increasing the availability to 95.5 percent), the savings would accumulate over a 30 day period to a 17 percent increase in availability. The increase in return-to-duty rates would be accomplished by reducing the time a soldier spends in administrative procedures.

Medical personnel interviewed stated that as many as 50 percent of war casualties may be saved if medical emergency data were readily available. Assuming casualty rates are 50 percent of the daily losses, a 50 percent increase in return would result in a 25 percent increase in daily availability or, for the assumed baseline, an increase of 48 percent on day 30 (21.4 percent to 31.8 percent).

The true value of SDT during a war needs to be quantified. However, the results of the analysis described in the above two paragraphs shows that a relatively small increase on replacement rates (combined return-to-duty, lives saved, quicker replacements due to proper identification) due to personnel and/or medical information will have a direct impact on personnel availability (e.g., .5 percent increase in daily availability produces 17 percent increase in personnel availability).

5.2 Results of the Peacetime Cost/Benefit Analysis

An objective of the CBA was to determine the best SDT concept options from a cost/benefit standpoint to feed into the overall selection process of this study. The results presented in this section first compare each concept by application and then the cumulative results for each of the three concepts are compared.

Each application, when analyzed separately, has "common costs" associated with the use of SDT. "Common costs" are costs that apply whether there is one application or a hundred applications for SDT. An example of such a cost is initial tags. Tags must be bought as long as at least one application is found for SDT.

"Common costs" are contained for each application investigated but are contained only once in the combined analysis. That is, the combined analysis is not the sum of the individual applications results. "Common costs" are added to the medical, personnel, and finance cost/benefits that result over and above the application costs. Table 1-1 in the C/B Appendix shows the breakout of costs/benefits by cost category and application. "C" stands for common cost. "M", "P", and "F" stand for medical, personnel, and finance cost/benefits.

An example of how common costs are used is in the personnel only application where columns "C" and "P" are summed. When combined applications are analyzed, columns "C", "P", "M", and "F" are summed even though the individual application results (like personnel just described) each include common costs.

5.2.1 Impact on Personnel Systems

Table 5.3 shows the dollars cost/benefits associated with a personnel application only of SDT. According to the CBA model, SDT2 has the highest payback with a benefit of \$743 million. SDT1 has a lesser payback of \$22 million, but is still beneficial. SDT2 would cost an additional \$80 million over the current methods. SDT3 costs are due primarily to the high cost of the tags themselves. More than one application must be found for SDT before SDT3 will become cost justified. However, SDT3 has the most space and, therefore, the most flexibility for multiple options.

TABLE 5.3. DOLLAR COST/BENEFIT RESULTS FOR PERSONNEL APPLICATIONS ONLY (x 1000\$)

	SDT1	SDT2	SDT3
R&D	2,000	2,275	2,275
Investment	9,132	72,109	442,794
O&S	<u>-25,794</u>	<u>-807,882</u>	<u>-355,303</u>
Total	-14,662	-733,498	+89,766

Personnel applications saved approximately 200 man-years/year for SDT1 and 5,000 man-years/year for SDT2 or 3. Even if only half of the personnel savings could be realized due to distribution, SDT1 would free up 100 administrative positions and SDT2 or 3 would free up 2,500 positions. The saved administrative positions could enhance the requirement to reduce support and increase combat positions for the Army of Excellence.

Time savings is another intangible resulting from peacetime application benefits. SDT1 saved an approximate work week per transaction. That is, an updated personnel file will be available an extra 40 work hours earlier with SDT1 on the average. SDT2 or SDT3 would reduce the processing time of a file by an average 63.5 work hours.

5.2.2 Impact on Medical Systems

Table 5.4 shows the dollar cost/benefits associated with a medical application only for SDT. SDT1 yields the highest benefit since only identification uses of the tag were captured for peacetime operations and SDT1 is the cheapest concept to achieve identification. Other peacetime benefits not captured in the CBA include the availability of medical records in locations where there are no current records (e.g., when someone is TDY, their record will be with them). However, wartime benefits of having a medical record readily available on a battlefield will not be realized with SDT1.

TABLE 5.4. DOLLAR COST/BENEFIT RESULTS FOR MEDICAL APPLICATIONS ONLY (x 1000\$)

	SDT1	SDT2	SDT3
R&D	2,000	2,275	2,275
Investment	28,192	102,500	473,185
O&S	<u>-404,921</u>	<u>-282,010</u>	<u>170,567</u>
Total	-374,729	-177,235	+646,027

SDT2 also yields a benefit which is approximately half of SDT1 benefits. However, SDT2 could provide a medical record on the battlefield. SDT3 again shows that one application for an expensive tag is impractical from a cost/benefit standpoint.

Medical applications saved approximately 1,000 man-years/year of administrative time. The savings is due to the personnel time saved in in-processing a soldier for medical treatment. Even if half of the savings can be realized, approximately 500 administrative positions could be freed up for combat positions.

According to a Battelle time and motion study, the average processing time savings is 14 minutes. That is, retrieving medical files would take an average of 14 minutes less administrative time than with the current methods. The large personnel savings resulting from 14 minutes is due to the large number of transactions that are accomplished per year (approximately 9 million).

5.2.3 Impact on Finance Systems

During the conduct of the CBA, limited data were available regarding financial peacetime benefits. Although a financial application concept for the SDT is now included in the Army's concept description, it was not available in time to be used in Battelle's study. Therefore, no quantitative analysis of the financial application is presented in this section.

Several areas of possible peacetime benefits that were identified in the finance area included:

- Payment record
- Casual payment record
- Authorization for payment
- Special pay records (e.g., record of jumps fed directly to finance)
- Scheduling for special pay requirements (e.g., commander has automatic schedule of who needs to jump).

5.2.4 Combined Peacetime Cost/Benefit Results

Table 5.5 shows an overview of the peacetime cost/benefit results. The first three columns are the results of the single application analyses. The last two columns show the cost/benefits of multiple applications.

The results show that SDT1 has the highest benefit for a medical only application, SDT2 is most beneficial for the personnel application, and no concept is viable for finance alone (until benefits are quantified). SDT3 is not cost effective for any of the single applications investigated.

All concepts are beneficial for multiple applications. This is due to the common costs being spread over the applications instead of being costed with each application. According to the CBA model, SDT2 shows the highest benefits, by orders of magnitude, over SDT1 and SDT3. However, the

TABLE 5.5. DOLLAR COST/BENEFIT RESULTS OVERVIEW (x 1000\$)

Application/ Concept	Medical Only	Personnel Only	M & P Combined	M, P, F Combined
SDT1	-374,729	-14,662	-411,350	-409,513
SDT2	-177,235	-733,498	-1,113,112	-1,109,417
SDT3	+646,027	+89,766	-289,848	-286,153

cost/benefits shown are for the applications investigated. The results show that additional applications for SDT may be more cost effective. SDT3 allows for the most expansion and may prove most cost effective in the long run.

Recommendations based on the CBA model only are:

- Continue development of SDT2 or SDT3 for medical/personnel applications
- Quantify finance benefits to determine if SDT is applicable
- Continue identification and marketing of other applications.

As a minimum, SDT2 should continue in development. However, due to the expandability allowed by SDT3, development of SDT2 should be done in a manner to allow an easy switch to SDT3 at a later date. That is, any constraints due to SDT3 should be taken into consideration in SDT2 development.

Finance applications for SDT need to be quantified. Currently, finance is not a justified application of SDT.

There is a large potential for using SDT for applications not investigated in this study. Training applications, loan records applications, identification applications, and others are all possible with SDT. Other applications may be added at a low cost (e.g., equipment, spares, software, and security) and will need low paybacks to break even. As other applications are identified, the SDT Program Office should determine which concepts could be used for the application and the costs/benefits should be updated for those concepts. This will provide the SDT Program Office with a rationale for choosing the final concept for procurement and for defining development requirements.

5.2.5 Wartime Analysis

A European war was assumed with one repository for the SDT data files. Tags would be read into the repository as soldiers arrive and all non-Geneva convention and nonemergency medical data would be erased. Such a procedure means that complete files (SDT files) are available for use in the theater of operation but the individual soldier will only carry identification and emergency medical information. Presently, without the SDT system, only

some of this data are currently available on the battlefield in any usable format. The primary uses of the tag would be:

- The medium to carry the soldier's file to the theater of operation
- Identification for a multitude of reasons
 - Casualty reporting and identification
 - Replacement operations
 - Medical, both preventative and emergency
 - File access (from repository)
 - Pay recording
- The only emergency medical data available on the battlefield in real time
- NBC contamination record (accumulative).

General assumptions that relate to the baseline for the cost/benefit analysis have been described in this section. Specific assumptions relating to one or two calculations are described in Appendix 1, Cost/Benefit Information, in the description of the calculation to which they relate.

5.3 Conclusions

There is a high potential for an SDT in both wartime and peacetime. The wartime benefits, although qualitative at this time, are very promising. Wartime benefits include higher return-to-duty rates, proper and quicker replacement of casualties, lives saved due to availability of medical records, alternative communications, and the creation/update of a theater-wide automated data system.

The peacetime benefits investigated are primarily the enhancements to the automated Army systems coming on-line. These enhancements include:

- Automatic retrieval of data files without keyboard data entry.
- Accessibility of data when the primary ADP system is unavailable.
- Transportation of machine readable data to new locations in a rugged format.

- Ability to handle last-minute unanticipated "diversions" of soldiers being transferred to new stations because the soldier carries his own file.

The automatic retrieval feature utilizes the SDT as a means of identification. An SDT will provide correct retrieval nearly every time. Currently identification must be verbally requested and keyed in for retrieval. Three aspects of possible error in the current method are: incorrect identification supplied, incorrect understanding of identification data, and miss hit keys on the keyboard. SDT will bypass such errors.

Accessibility of data in austere areas is another enhancement of the SDT. An SDT will be available even if an automated system is unavailable. A soldier who is reassigned on the battlefield will carry his own file. The automated systems may not be able to be updated in real time during war. The SDT will allow local automated files to be created quickly, and in the event of computer destruction, will provide a backup data file. This aspect of SDT may be crucial for emergency medical in both wartime and peacetime. Army personnel entering facilities away from their station will have a backup file with them that will provide emergency information and enough identification to locate the automated file.

SDT may also be used as a data carrier in both wartime and peacetime. Tactical and strategic plans may be carried on SDT when communication lines are tapped, cut, or jammed. A soldier caught wearing an SDT will not be an obvious carrier if all personnel are so equipped. During peacetime the tag could be used to carry data for reassignment. Clerk time will be cut for outprocessing and inprocessing by use of the SDT as a "traveling" data file.

Medical and personnel applications were recommended as a result of the CBA. Indications are that other beneficial applications may be and should be encouraged in order to increase the number of benefits as compared to cost. Examples of such applications are:

- As a loan record or receipt for equipment
- As a training record (attendance and qualification)
- As a jump record (attendance)
- As a record of nuclear, biological, or chemical contamination
- As a meal card or ration card.

Such applications would have minimal cost to add to an existing SDT with enough capacity and the benefits may be large.

A conclusion that is drawn from the use of multiple applications is that a higher capacity tag is probably indicated. (Note that this is only the case if the additional applications cannot be supported by the data already carried on the tag. In some instances, particularly identification, the same data can be utilized.) A low capacity SDT may restrict the potential benefits that may finally be realized.

In summary, the SDT may provide some wartime benefits, and will definitely have peacetime benefits (for medical/personnel application). Lastly, the Army needs to quantify the effects of SDT on the battlefield. The updating of planned automated systems during wartime will be cumbersome to create and update without SDT.

6.0 INTERACTION WITH EXISTING OR PLANNED ADP SYSTEMS

A major consideration of the Soldier Data Tag System is the need to interface with a variety of ADP systems. Within the Army this need is highlighted by the fact that most existing personnel, financial, and medical systems operate independently and on different hardware. However, the SDT concept is not restricted to the Army alone. Other service branches within DoD have data and processing requirements similar to those found in the Army. Because of the great potential for applying the SDT technology outside the Army, corresponding systems in the Navy, Air Force, and the Marines were studied from a compatibility viewpoint.

Throughout DoD many new systems are now being planned and developed and some old ones are being enhanced. In addition, new hardware is being procured to replace older terminals and computers. The need for the SDT to effectively interface with these systems is obvious. But, to be most effective, SDT specifications must be incorporated into the design of these systems.

This section addresses the specific issues of military ADP systems today and over the next several years as they relate to SDT compatibility. The section is divided into the following subsections:

- **6.1 Compatibility Issues.** What constitutes system compatibility?
- **6.1.1 Existing and Planned ADP Systems.** Discussion about those DoD systems with which SDT would likely interface. (Pertinent data tables are located at the end of this section.)
- **6.1.2 Soldier Data Tag Software Requirements.**
- **6.2 SDT Attitudes and Opinions.** Attitudes and opinions in the DoD Software Applications Community.
- **6.3 Conclusions.**
- **6.4 Recommendations.**

6.1 Compatibility Issues

In order to determine whether the SDT is or is not compatible with a particular application system or hardware configuration it is first necessary

to define what is meant by "compatible". The SDT can be considered compatible with an application when said application is able to read data from the tag and/or write data to the tag. This statement carries with it the implicit assumption that a link between the application's hardware and the SDT tag interface device has been established.

To determine whether the SDT can interface to a specific application and to decide what level of effort may be required, several questions need to be answered:

- Does the application hardware have any available RS232 ports into which the SDT tag interface device can be attached?
- Can the necessary communications protocol be set up in the applications hardware to read and write the tag?
- What type of modifications are necessary (e.g., software, firmware, hardware) to effect a workable physical interface?
- Can application software be readily modified to accommodate user requirements for the SDT?

The following discussion addresses these questions.

For the SDT to interface with existing or planned application systems a physical link must be established. This link can be made on today's hardware if the necessary RS232 port is available. It is not known how many of today's terminals have available RS232 ports and thus are capable of interfacing with SDT. What is known, however, is that the TACCS (Tactical Army Combat Service Support Computer System) computer, which is scheduled for deployment this year, does have several available RS232 ports and has been interfaced with the SDT tag interface device. The TACCS is a microcomputer capable of operating either in a stand-alone mode or as a terminal to a mainframe. Current Army applications, such as SIDPERS (Standard Installation/Division Personnel System), are being enhanced to run on the TACCS. Applications now under development, such as TAMMIS (Theater Army Medical Management Information System) and CAMIS (Continental Army Management Information System), are being specifically engineered to run on TACCS. In the other services a similar movement to microcomputers is occurring. For the SDT system development, this means that a physical link to most ADP systems will be possible.

Once a physical link has been established, the necessary communication between the SDT tag interface device and the hardware must be made. A common concern here relates to the character size. Should the SDT tag interface device send and receive 7- or 8-bit characters? The prototype SDT system used an 8-bit character sandwiched within start, stop, and parity bits. Most hardware that provides an RS232 port can support both 7- and 8-bit character communication. Establishing one or the other is generally accomplished via software or function keys on the terminal or hardware in question. The 8-bit character form adopted by Datakey in their prototype SDT tag interface device can be interfaced to most hardware in use today or planned for the future. In any case, opting for a 7-bit character, or some other form, does not make the interface job any easier, and in fact will cut the available character set in half. Although there is no industry standard, per se, the 8-bit character appears to be a workable entity. The trend toward microcomputers like the TACCS or IBM PCs will have a positive impact on the SDT's ability to interface with various application systems. **Battelle recommends that the 8-bit character be established as the SDT standard character size.**

The level of effort required to establish the communications interface will, of course, depend upon the particular hardware in question. The new microcomputers and many older intelligent terminals can effect a workable physical interface via function keys or through modifications to software. This is generally straightforward and inexpensive. Some equipment, however, may require additional firmware or hardware retrofits in order to establish the proper interface to the SDT tag interface device. This can be time consuming and expensive. New equipment procurements will continue to reduce the significance of this issue. Assuming that the trend for high awareness of needs for communication interfaces continues, most new equipment will be configured for ready use of devices such as the tag interface device.

Assuming that an appropriate communications linkage has been established for the SDT, a remaining compatibility issue is the application software with which the tag must interface. User requirements within each functional discipline will dictate how the tag is to be utilized. Obviously, existing applications will require modifications to accommodate SDT. New applications can have the necessary SDT interface incorporated into their design. Applications were not examined in this study to determine how readily

they would work with the SDT; however, it is clearly advantageous to establish SDT requirements as soon as possible in an application's development life cycle.

6.1.1 Existing and Planned ADP Systems

With compatibility issues generally established, it is necessary to look at existing and planned ADP systems and determine specific SDT interface requirements. For the purpose of this study, ADP systems were limited to major applications in the functional areas of Personnel, Finance, and Medical. Information was gathered from the four service branches (Army, Navy, Air Force, and Marines) and the three components within each (Active, Reserve, National Guard) where appropriate and available. The Army identified several of its systems to be included in the study. These were JACS, SIDPERS, TAMMIS, and TRIMIS for the Active Army, and CAMIS for the Army Reserve and National Guard. Several initial points of contact were provided for the other service branches. Table 6.1 identifies the current and planned ADP systems included in this study. Several other ADP systems were also identified, but limited documentation was available at the time of the study. Table 6.2 (located at the end of this section) summarizes the results of the information search where each page in the table describes ADP applications and hardware for a given military branch, component, and functional concern. Whenever sufficient data is present, specific comments on SDT compatibility are made.

Several statements about the data collection process are in order. Most of the information was obtained through telephone interviews with key application personnel (generally, program or project managers). Hard copy documentation was not readily available, usually because it contained procurement sensitive material. The documentation that was obtained is listed in the bibliography at the end of this section. Detailed data on unit-level hardware configurations outside the Army was sketchy at best; however, general descriptions by PMs indicated that other service branches have hardware similar to the Army's.

TABLE 6.1. CURRENT AND PLANNED ADP SYSTEMS

		Army	Navy	Air Force	Marines
Active	P	SIDPERS RAPIDS	MAPMIS RAPIDS	ADPS RAPIDS	MMS RAPIDS
	F	JACS	JUMPS-Navy	JUMPS-Air Force	JUMPS-Marines
	M	TAMMIS TRIMIS	TRIMIS	TRIMIS APES	
Reserve	P	CAMIS			REPMIS
	F	CAMIS	RPSI	ARPAS	
	M				
National Guard	P	CAMIS			
	F		RPSI	ARPAS	
	M				

P - Personnel systems.
 F - Financial systems.
 M - Medical systems.

6.1.2 Soldier Data Tag Software Requirements

The software requirements of the Soldier Data Tag system relate to three distinct system components: the tag interface device, the terminal interface, and the application. Requirements for the tag interface device determine the nature of the program logic that directly controls the reading and writing of the SDT. Terminal interface requirements define the communications protocol necessary to permit interaction between a terminal device and the SDT tag interface device. Application requirements determine what, how, when, and where specific application data is to be read from or written to the tag.

Software requirements for the SDT are closely related to the system compatibility issues described at the beginning of this section. The three software components must play together to permit the proper functioning of the SDT system.

Requirements for a prototype tag interface device are currently established. These requirements specify an 8-bit character form for serial I/O and direct a Portable Data Base Manager (PDBM) which automatically organizes data into records or files. As detailed in the Compatibility Issues subsection, Battelle recommends that the Army use this 8-bit character for the SDT system.

Requirements for the terminal interface are not as clearly defined, but should adhere to the following guidelines:

For existing equipment--

- the terminal device should have sufficient serial I/O capacity (i.e., it should have at least one RS232 port available for use with the SDT tag interface device)
- the terminal should be programmable via function keys or software modifications to permit proper communication with the SDT tag interface device. Most terminals of this type will handle either 7- or 8-bit character forms.

For new procurements--

- the terminal device should be required to directly interface with a selected SDT tag interface device and have sufficient I/O capacity to handle future needs during its useful life
- the terminal should readily permit modifications to its communications protocol to permit different SDT configurations, including 7-bit characters or nonserial communications.

Application software was not specifically analyzed in this study; however, several statements can be made with regard to requirements. Existing application software poses the greatest problem for the SDT. These systems were not designed with the tag in mind and, as such, may not be amenable to change. Requirements for SDT compatibility must take into account feasibility and cost for each system being considered. Future applications and those

currently under development should have the capability of interacting with SDT designed into them, even if the SDT will not be used immediately. The entire area of SDT application requirements should be studied in detail. The future success of the Soldier Data Tag will depend greatly on how well it addresses the users' needs. Many systems are now being developed or enhanced in all DoD service branches. **The Army should move to establish SDT standards and requirements as quickly as possible.**

The preceding discussion on software requirements and SDT compatibility certainly apply for tags with memory sizes up to 64,000 bits. For alternative SDT configurations, such as larger capacity tags, the same communication mechanism can be used; however, data access time will be directly related to memory size. If faster data access times are required, the prototype asynchronous form of communication may not be appropriate. The impact on the SDT due to a different form of communication was not studied; however, the software requirements for the tag interface device and the hardware interface protocol would differ greatly from those described above.

6.2 SDT Attitudes and Opinions

An important offshoot of the data collection process for SDT system compatibility were the opinions and attitudes of the interviewees. Most of those interviewed had heard of the Soldier Data Tag program, and some were very knowledgeable about it. However, more important than simply knowing about the SDT system was the fact that most had definite feelings, opinions, and concerns, and a desire to share those attitudes. Many of the opinions were very positive, some were middle-of-the-road, and a few were negative. Although personal attitudes about SDT do not directly relate to system compatibility, they often represent a general consensus which may indicate the degree of support that can be expected from a particular group. Battelle believes that the Soldier Data Tag program can benefit from this knowledge by preparing itself to address these sometimes intangible issues.

Across all DoD service branches, including the Army itself, the personnel community has the greatest difficulty with the SDT concept. Within the Army the personnel function is embodied mainly in the SIDPERS system. SIDPERS 3 is scheduled to be operational in 1989. Developers of the system

feel that SDT has limited value since SIDPERS 3 will provide online, real time access to a central data base for all personnel requirements by simply keying a soldier's SSN. For combat situations a portion of the data base can be downloaded to a TACCS computer for field use. The tag is viewed as useful for ID purposes and to store or transfer, within a unit, locally unique data which is not required or maintained on a central data base.

The Navy personnel community views the SDT in a little different way. The Navy has the lead role in the development of the RAPIDS (Realtime, Automated Personnel Identification System) program for all DoD service branches. Although the purpose of RAPIDS is different than that of SDT, its developers view the tag as competitive rather than complementary to the RAPIDS card. The SDT program needs to overcome this image, which is particularly prevalent in the personnel communities of all DoD service branches, and present a solid case based on the merits of the SDT program.

The Air Force, seeing drawbacks in the RAPIDS card, is planning their own test of an Individual Data Storage Device (IDSD). The Air Force envisions a system which is strictly for personnel processing, dealing with such issues as shots, wills, training, and squadron deployment. With proper cultivation, the SDT might very well be able to fill the role of the IDSD and reduce duplication of effort as well.

The Marines have needs which differ sharply from the other branches. They need to keep track of many people rapidly moving from one location to another. Generally, the Marines require equipment that is more rugged than other branches. The physical specifications for the SDT system would probably meet the Marines requirements. However, in a combat environment, it was generally believed that the tag would not enhance current capabilities to identify casualties.

The financial community tended to be fence-sitters in their attitudes toward the SDT program. Their enthusiasm for a device which could be used for recognition purposes or used with Automatic Teller Machines was tempered by their concern over the security of their financial system.

All service branches use some form of JUMPS (Joint Uniform Military Pay System) to process payroll, taxes, and other personnel financial records. But, alas, the system is neither joint nor uniform, and so SDT means something different to everyone. The Army has specific limitations on the use of their

HP 3000 JUMPS input terminals. It is unlikely that SDT would be permitted to interface to the Army financial system through these terminals. Such an interface may occur through TACCS to TAFIS. The Navy, on the other hand, appears to be very interested in SDT developments and are waiting to see what happens. They are not sure exactly how they would use the tag, but wish to see what direction the Army is going in this matter before they make any commitments. The Air Force appears to have the most advanced automated financial system of all service branches. They are very interested in the SDT concept and see definite uses for such a device for such things as TDY cash advances, rental cars, and housing--especially if the main system is temporarily down.

The SDT program garners its greatest support from the medical community. The general consensus across all DoD service branches is that the tag has value both in peacetime and wartime for medical purposes. Of some importance, and worth noting here, were two concerns from the TRIMIS program office. First, there is no clear specification of how the SDT system would interface to TRIMIS. Second, once an interface was established, they expressed a concern regarding the ability to keep the data on the tag current. The Army has a liaison medical officer familiar with the SDT system who is currently working with the TRIMIS development team. This should allow the Army to address these concerns quickly and to assume an active role in incorporating the SDT concept into the TRIMIS design. TRIMIS offers a good stepping stone for the introduction of SDT into other service branches since it truly represents a cooperative effort among the services.

6.3 Conclusions

The following conclusions can be drawn from Battelle's study of SDT system compatibility:

- The software requirements adopted for the prototype SDT system will provide a compatible interface to existing and emerging ADP systems.
- An 8-bit character size is no less compatible than the 7-bit size and offers an expanded character set.

- Many people in the studied ADP community know something about the Soldier Data Tag, which is a credit to the SDT program staff. The greatest support comes from the medical arena, followed by the financial area and personnel.

6.4 Recommendations

With the above in mind, Battelle recommends that the Army:

- Adopt the 8-bit character form for serial I/O processing of SDT data.
- Identify all candidate terminals for SDT interface in DoD and determine the level of effort required to achieve the needed communications linkage.
- Establish SDT application software requirements as quickly as possible.
- Identify existing applications that will interface with SDT and determine their compatibility constraints.
- Incorporate SDT standards and requirements into all new application software development within DoD.
- Develop or expand a list of user needs for SDT in each functional discipline and aggressively sell the SDT concept based upon its ability to meet those needs.
- Pursue specific opportunities related to the tri-service development of the TRIMIS system to establish the SDT in other services.

TABLE 6.2. SDT SYSTEM COMPATIBILITY
 SERVICE: Army (Reserve)
 FUNCTIONAL AREA: Personnel Financial

System	Description/Equipment	Date	Comments
CAMIS	Continental Army Management Information System	FY 86	Prototype.
		2nd Qtr FY 87	First test of production system.
		FY 89	Completely deployed and operational.
DARMS	Developmental Army Readiness and Mobilization System	Operating	Interim system until CAMIS is ready (used to be called DCVS).
<u>Hardware Data</u>			
	CAMIS hardware not yet known	Not known	
(DARMS)	Wang VS 100 Wang 275 - Dumb terminals used for data I/O	Operating Operating	One located at each CONUSA. 250 terminals at the various Reserve components. Most using dial-up RS232 connections.
<u>SDT Compatibility</u>			
Number Available RS232 (serial)	Character Size (bits)		Comments
			Plans call for CAMIS to interface with a unified Army personnel data base when SIDPERS-3 is available.

TABLE 6.2. (Continued)
 SERVICE: Army (Active)
 FUNCTIONAL AREA: Financial

System	Description/Equipment	Date	Comments
<u>Application Data</u>			
JACS	JUMPS-Army Automated Coding System	Operating	Used to process Active Army pay information. Handles tax accounting for Army Reserves. Although operational, new or modified modules such as the separation module continue to come on line regularly.
(JACS)	UNIVAC 1100 HP 3000 Series 30 used to input pay information	Operating Operating	One centrally located system. 25 systems are now in use.
<u>Hardware Data</u>			
<u>SDT Compatibility</u>			
Number Available RS232 (serial)	Character Size (bits)	Comments	
		JACS terminals have been specifically designated for use with JACS processing only. Interface to SDT might eventually be possible using an Automated Teller Machine concept.	

TABLE 6.2. (Continued)

SERVICE: Army (Active)
 FUNCTIONAL AREA: Personnel

System	Description/Equipment	Date	Comments
<u>Application Data</u>			
SIDPERS 2	Standard Installation/Division Personnel System-Module 2	Operating	Batch processing - data input via card image format. Separate Unit data bases are maintained.
<u>Hardware Data</u>			
DAS-3	Decentralized Automated Service Support System - Honeywell mini (47)	Operating	Van-based system for field use. Being phased out.
VIABLE	Mainframes: Amdahls' and IBM	Operating	
<u>SDI Compatibility</u>			
Number Available RS232 (serial)	Character Size (bits)		Comments
			No clear interface to SIDPERS data is available at the Module 2 level.

TABLE 6.2. (Continued)

SERVICE: Army (Active)
 FUNCTIONAL AREA: Personnel

System	Description/Equipment	Date	Comments
<u>Application Data</u>			
SIDPERS 2.5	Standard Installation/Division Personnel System-Module 2.5	4th Qtr FY 85	Permits an extract of SIDPERS data base to reside on a unit's TACCS. Data available for ad hoc inquiry. Data input for SIDPERS transactions using TACCS. SIDPERS 2.5 will only run on the TACCS.
<u>Hardware Data</u>			
TACCS	Burrough's B26 system (16 bit micro)	4th Qtr FY 85	Completely portable. The TACCS will batch SIDPERS data entry transactions for later submission to VIABLE or DAS 3. SIDPERS processing and file structure will remain the same, however, data for all units using SIDPERS 2.5 will be merged.
DAS 3	Honeywell mini	Operating	
VIABLE	IBM or Amdahl mainframe	Operating	
<u>SDT Compatibility</u>			
Number Available Character Size			
RS232 (serial) (bits)			
Several	7 or 8		TACCS--programmable to handle either 7 or 8 bit characters from a serial I/O device. SDT read/write interface to TACCS has been demonstrated.

TABLE 6.2. (Continued)

SERVICE: Army (Active)
 FUNCTIONAL AREA: Personnel

System	Description/Equipment	Date	Comments
SIDPERS 2.75	Standard Installation/Division Personnel System-Module 2.75	FY 86 to FY 88	Represents the automation of many unit personnel functions such as Personnel Management, Actions, Record Keeping, and Administration. Makes use of information available because of SIDPERS 2.5. Fielding of SIDPERS 2.75 will be completed over a two year period as functions are available.
<u>Application Data</u>			
<u>Hardware Data</u>			
TACC	Burrough's B26	4th Qtr FY 85	
<u>SDI Compatibility</u>			
Number Available RS232 (serial)	Character Size (bits)		Comments
Compatibility through TACCS (see SIDPERS 2.5).			

TABLE 6.2. (Continued)
 SERVICE: Army (Active)
 FUNCTIONAL AREA: Personnel

System	Description/Equipment	Date	Comments
SIDPERS 3	Standard Installation/Division Personnel System-Module 3	<u>Application Data</u> FY 87	Phase I - Current SIDPERS, establish ADR DBMS (relational) on VIABLE.
		FY 88	Phase II - New structured, interactive SIDPERS, phase DAS 3 out.
		FY 89	Phase III - Merge Reserves and National Guard data base with Active Army to form a Total Army data base.
TACCS	Burrough's B26 micro	<u>Hardware Data</u> 4th Qtr FY 85	
VIABLE		Operating	
DDN	Defense Data Network	Not known	A standard, integrated network probably operational when SIDPERS 3 Phase III is available.
<u>SDI Compatibility</u>			
Number Available RS232 (serial)	Character Size (bits)	Comments	
Compatibility through TACCS (see SIDPERS 2.5).			

TABLE 6.2. (Continued)

SERVICE: Army (Active)
FUNCTIONAL AREA: Medical

System	Description/Equipment	Date	Comments
	<u>Application Data</u>		
TAMMIS	Theater Army Medical Management Information System	1st Qtr FY 86 1st Qtr FY 87	Prototype fielded by early FY 86. Initial deployment of operational system by early FY 87. Totally fielded in 2-1/2 years. Will interface to TRIMIS. Plans call for an eventual interface to SIDPERS data base.
	<u>Hardware Data</u>		
TACCS	Burrough's B26 micro	4th Qtr FY 85	DAS 3 was to be used for logistics portion of TAMMIS. MEDLOG subsystem has removed the need for DAS 3.
ULC	Unit Level Computer - hardware not known	Not known	Planned to interface with systems above and below.
(T) LOGMARS	Hand held device	FY 86	
	<u>SDT Compatibility</u>		
Number Available RS232 (serial)	Character Size (bits)	Comments	
4	7 or 8	Compatibility with TACCS.	
1 or 2	Not known	ULC - SDT interface not yet established.	
Not known	Not known	Hand held device - SDT reading should be possible.	
1	Not known		

TABLE 6.2. (Continued)

SERVICE: Army/Navy/Air Force (Active)
 FUNCTIONAL AREA: Medical

System	Description/Equipment	Date	Comments
	<u>Application Data</u>		
TRIMIS	Tri-Service Medical Information System		TRIMIS composed of 4 separate projects--two have definite SDT applicability:
		1st Qtr FY 86	AQCESS (Automated Quality of Care Evaluation Support System). This is on interim system to be operational by early FY 86. Software development underway.
		1st Qtr FY 87	CHCS (Composite Health Care System). RFP for complete system to be released in April 85. Initial deployment in early FY 87.
	<u>Hardware Data</u>		
(AQCESS)	Micro or mini (hardware selection in April 85)	Not known	Hardware must be ready for system deployment in early FY 86.
(CHCS)	Not known	Not known	
	<u>SDT Compatibility</u>		
	Number Available RS232 (serial)	Character Size (bits)	Comments
	Not known	Not known	A prime focus of the TRIMIS Program Office is on defining necessary interfaces between TRIMIS and other systems such as SDT and RAPIDS.

TABLE 6.2. (Continued)

SERVICE: Navy (Active)
 FUNCTIONAL AREA: Personnel

System	Description/Equipment	Date	Comments
	<u>Application Data</u>		
MAPMIS	Manpower and Personnel Management Information System	Operating	
	<u>Hardware Data</u>		
(MAPMIS)	IBM 3033's, 4341's, 4361's SNA architecture. Uses MVS operating system. Uses TOTAL, ADR, Cullinet DBMS's	Operating	Plan to stay with current configuration for next 4 to 5 years. These machines are located at a central site.
DDN	Defense Data Network	Not known	A standard, integrated military communications network.
	<u>SDT Compatibility</u>		
	Number Available RS232 (serial)	Character Size (bits)	Comments
	Not known	Not known	Asynchronous communications through a front end processor would be possible. It is not known what equipment is available to field units which might interface with SDT.

TABLE 6.2. (Continued)

SERVICE: Navy, Army, Air Force, Marines (Active)
 FUNCTIONAL AREA: Personnel

System	Description/Equipment	Date	Comments
	<u>Application Data</u>		
RAPIDS	Realtime, Automated Personnel Identification System	FY 87	Full deployment completed in FY 87. Navy is taking the lead in system development, but RAPIDS will cross all DoD service branches when fully deployed.
(RAPIDS)	Not known (micro's or mini's and dumb terminals)	3rd Qtr FY 85	Hardware selected will provide consistency across all military branches.
	<u>Hardware Data</u>		
	<u>SDT Compatibility</u>		
Number Available RS232 (serial)	Character Size (bits)	Comments	
Probably several	Probably 7 or 8	Selected equipment should be programmable to interface with the SDT tag interface device.	

TABLE 6.2. (Continued)

SERVICE: Navy (Active)
 FUNCTIONAL AREA: Financial

System	Description/Equipment	Date	Comments
	<u>Application Data</u>		
JUMPS-Navy	Joint Uniform Military Pay System - Navy	Operating	Currently a pay forecast is sent to pay offices around the country. By early FY 86, more than 100,000 personnel in CONUS will be paid directly from the central site via the Federal Reserve EFT.
	<u>Hardware Data</u>		
(JUMPS)	IBM 3081 and others	Operating	The JUMPS-Navy application shares the processors with the personnel office of the Navy.
DDN	Defense Data Network	Not known	Initial tests at a Navy test site to begin by Summer 85.
	<u>SDT Compatibility</u>		
Number Available RS232 (serial)	Character Size (bits)	Comments	
Not known	Not known		

TABLE 6.2. (Continued)

SERVICE: Navy (Reserve)
 FUNCTIONAL AREA: Financial

System	Description/Equipment	Date	Comments
RPSI	Reserve Pay System Improvement	Operating	Handles pay processing for the Naval Reserve.
(RPSI)	IBM 3081	Operating	Shares processors with JUMPS-Navy.
<u>Application Data</u>			
<u>Hardware Data</u>			
<u>SDI Compatibility</u>			
Number Available RS232 (serial)	Character Size (bits)	Comments	
Could not determine compatibility.			

TABLE 6.2. (Continued)

SERVICE: Air Force (Active)
 FUNCTIONAL AREA: Personnel

System	Description/Equipment	Date	Comments
	<u>Application Data</u>		
APDS	Advanced Personnel Data System	Operating	
	<u>Hardware Data</u>		
(APDS)	Burrough's 3547 100 series Sperry 1160 Four Phase IBM System 1 supporting IBM PC's in various work centers	Operating	The Air Force is currently deciding whether to continue with a variety of processors or to establish a single, standard unit.
	<u>SDI Compatibility</u>		
Number Available RS232 (serial)	Character Size (bits)	Comments	
Not known	7 or 8	IBM PC's can accommodate either 7 or 8 bit characters and could support the prototype SDI tag interface device.	

TABLE 6.2. (Continued)
 SERVICE: Air Force (Active)
 FUNCTIONAL AREA: Medical

System	Description/Equipment	Date	Comments
<u>Application Data</u>			
Not known			Beyond TRIMIS (see page ___), the Air Force seems to have no general medical information system.
APES	Automated Patient Evacuation System	Not known	This system appears to be tactical in nature. No additional information has been obtained.
<u>Hardware Data</u>			
	Not known		Not known
<u>SDI Compatibility</u>			
Number Available RS232 (serial)	Character Size (bits)		Comments
Not known	Not known		

AD-A169 564 SOLDIER DATA TAG STUDY EFFORT(U) BATTELLE COLUMBUS LABS 3/3
OH R D ROSEN ET AL. 10 JUN 85 DDTB60-84-C-0146

UNCLASSIFIED

F/G 6/5

NL



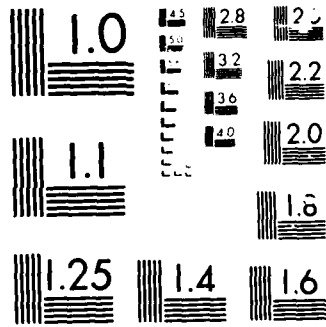


TABLE 6.2. (Continued)

SERVICE: Air Force (Active)
FUNCTIONAL AREA: Financial

System	Description/Equipment	Date	Comments
JUMPS-Air Force	Joint Uniform Military Pay System - Air Force	Operating	The Air Force currently pays 90.3% of personnel through EFT. Air Force system is quite similar to Navy system and runs on Amdahl computers which are compatible to the Navy IBM machines. Air Force and Navy are establishing an agreement in principle to use each other's computers for backup purposes.
(JUMPS)	Amdahl 5870, 5850 New Amdahl as powerful as the two current machines Major upgrade planned Four Phase	Operating FY 86 FY 87 Operating Operating	These large mainframes centrally located at the Air Force Accounting and Finance Center. The computer systems are available at the Base Level. 1160's incrementally being brought online through early FY 87.
	Sperry 1160 Burrrough's 3500 System 11 (Sperry mini)	Operating Operating	System 11 available in Base accounting offices.
<u>SDI Compatibility</u>			
Number Available RS232 (serial)	Character Size (bits)		Comments
Not known	Not known		

TABLE 6.2. (Continued)

SERVICE: Air Force (N. G./Reserve)
 FUNCTIONAL AREA: Financial

System	Description/Equipment	Date	Comments
	<u>Application Data</u>		
ARPAS	Air Reserve Pay and Allowance System	Operating	
	<u>Hardware Data</u>		
(ARPAS)	Uses same equipment as the active component HP 3000	Operating 4th Qtr FY 85	This system will be used to handle some 20,000 transactions per month rejected from ARPAS and JUMPS because of data errors.
	<u>SDT Compatibility</u>		
Number Available RS232 (serial)	Character Size (bits)	Comments	
Not known	Not known		

TABLE 6.2. (Continued)

SERVICE: Marines (Active)
 FUNCTIONAL AREA: Personnel

System	Description/Equipment	Date	Comments
	<u>Application Data</u>		
MMS	Manpower Management System	Operating	MMP share computer resources with JUMPS-Marines.
	<u>Hardware Data</u>		
(MMS)	Amdahl (IBM 370 compatible)	Operating	Mainframe located centrally at the Marine Corp Finance Center.
	IBM 3270	Operating	Each regional Data Processing Installation has various terminal hardware that it uses to interact online with an integrated JUMPS/MMS data base.
	IBM PC's, other micros (3270 emulation)	Operating	
	Dumb terminals	Operating	
	<u>SDT Compatibility</u>		
Number Available RS232 (serial)	Character Size (bits)	Comments	
Some available	7 or 8	Those terminals with available RS232 ports can be programmed to support the SDT tag interface device.	

TABLE 6.2. (Continued)
 SERVICE: Marines (Active)
 FUNCTIONAL AREA: Financial

System	Description/Equipment	Date	Comments
	<u>Application Data</u>		
JUMPS-Marines	Joint Uniform Military Pay System - Marines	Operating	JUMPS has been online since the early 1970's.
	<u>Hardware Data</u>		
(JUMPS)	Amdahl (IBM 370 compatible)	Operating	Shares processor with the Personnel functional area.
	IBM 3270	Operating	Online interaction with an integrated JUMPS/MMS data base located at the Marine Corp Finance Center.
	IBM PC's, micros	Operating	
	Dumb terminals	Operating	
	<u>SDT Compatibility</u>		
Number Available RS232 (serial)	Character Size (bits)	Comments	
Some available	7 or 8	Those terminals with available RS232 ports can be programmed to interface to the SDT tag interface device.	

TABLE 6.2. (Continued)

SERVICE: Marines (Reserve)
 FUNCTIONAL AREA: Personnel

System	Description/Equipment	Date	Comments
	<u>Application Data</u>		
REPMS	Reserve Personnel Management Information System	Operating	
	<u>Hardware Data</u>		
(REPMS)	Processing equipment shared with active component	Operating	
	<u>SDT Compatibility</u>		
Number Available RS232 (serial)	Character Size (bits)		Comments
Not known	Not known		

7.0 CONCLUSIONS AND RECOMMENDATIONS

Presented below are a set of conclusions from the study effort. These discussions are repeated at the end of the appropriate sections and are included here for convenience.

7.1 Conclusions

7.1.1 Security Issues

It is useful at this stage of the SDT's life cycle to examine potential countermeasures to the data security threat. On the other hand, the intermediate state of the SDT concept makes it impossible at this time to recommend categorically the specific use of some of the various security tools that have been described in this chapter, nor to absolutely evaluate the level of security obtainable in the ultimate system. As indicated, a variety of techniques are available, both technical and operational, which can be applied to protect against given threats. Before stating our conclusions with respect to the overall issue of SDT system security, it is useful to note some specific recommendations.

It is crucial that the threat to the SDT system be continually reevaluated:

- As the design of the SDT system evolves
- Whenever a new application is proposed for the fielded system
- Whenever there is a change in the technology or configuration in the fielded system
- Periodically to reevaluate new technological tools available to potential system penetrators.

While there are technological countermeasures, it is apparent that operational countermeasures will also need to be employed. Examples of where operational safeguards will probably have to be employed include:

- In the design process, to insure that a combination of compartmentalization and independent review prevents the inclusion of "trap doors" which could be utilized for future penetrations

- In the distribution process, where tracking techniques will be needed to insure that counterfeit tags are not injected into the pipeline
- In the control and utilization of terminals in the deployment process, to insure that terminal sabotage does not cause critical delays or confusion
- In the system support phase, where configuration control techniques will be needed to insure that new applications do not accidentally or intentionally damage or penetrate the system
- In the auditing process, where covert checks can be made to insure that the contents of individual tags still match the approved data maintained centrally.

As indicated above, while not possible to be categorical with respect to the set of technological countermeasures which should be employed within the SDT system, there are nevertheless some likely choices to highlight:

- It is unlikely that security in such a widely distributed and publicized system can be maintained through the use of "secret" passwords, encryption algorithms, or integrated circuit design. Instead, near-term solutions will most likely involve:
 - the use of public key method of data encryption
 - the use of a robust hardware architecture with some capability for electronic destruction of critical data paths.
- It is unlikely that an absolutely foolproof techniques will be found to guarantee the protectability of militarily-critical information in the tag. This means that:
 - operational approaches will be needed to protect information on the tag needed on the battlefield and of military importance to the enemy
 - attention will have to be paid to human factors so that the soldier will in general not want to discard the tag in combat.

It should be noted that the inability to guarantee the security of classified information is not a special weakness of the SDT; the same is true of information that is carried into battle in the heads of soldiers. All that

can be done is to make it difficult (though not impossible) to obtain, and to parcel the information out so that the loss of one part of it does not compromise the whole.

In conclusion, while it will not be possible to guarantee the security of data contained in the SDT system, or the integrity of the system itself, a combination of the technological opportunities presented by the tag, the array of operational safeguards which could be employed, careful consideration of data and applications to be implemented using the tag, and care in the partitioning of militarily significant data will likely provide an adequately secure and militarily useful system.

7.1.2 Component Design Issues

Based on the previous discussions regarding the physical design of the SDT system, several conclusions can be reached. First, regarding the information storage technology for the SDT, both electrically erasable memory (EEPROM) and the optical stripe appear to have attributes which satisfy the basic requirement for the tag. However, the survivability of an optical stripe and the associated interface device in the envisioned battlefield environment is uncertain. The EEPROM has a longer track record, low cost, and demonstrated survivability. If a rapid fielding of the soldier data tag system is to be accomplished, then the most logical choice is the use of a EEPROM/processing structure based on the prototype systems. It should be noted, however, that the current system still needs rigorous testing and design revisions in order to result in a design which meets the Army's overall requirements now and in the future.

From the information previously presented in the materials section, it can be concluded that **a polymeric encasement is the most probable approach to an effectively operational SDT.** Through understanding the critical importance of the survivability of the SDT in the battlefield, it can be concluded that **the mechanical properties are the least important requirements to be met, with the most important requirements being physical, electrical, and chemical properties.** These requirements can most probably be met by two of the candidate materials: liquid crystal polymer (LCP) and polyphenylene sulfide (PPS). therefore, they should be considered as viable polymers for the SDT application.

Based on the materials and processing cost/benefit analysis, it is expected that the equipment life will be diminished by at least half, and utility costs will double with the use of PPS. As a result of the estimate of materials, utilities, and labor costs, the total unit cost for the SDT made from PPS is only 4 cents/unit more than compared with the costs of a SDT made from LCP. However, a greater savings may be realized by the use of LCP if equipment life and costs are taken into account.

Finally, in a tactical situation the SDT would be difficult to detect by any of the following methods: IR photography, chemical, sound, electronic, or radar reflectance. In addition, there are several viable printing techniques which can be used in the field to apply surface information to the SDT. These printing methods could include either a reverse coating or electrophotographically imaging the required information on a film then laminating it to the SDT. Such applications are fast and relatively simple; the equipment should be quite mobile; and the lamination will provide mechanical and chemical protection for the surface information.

It is our opinion the concept of the SDT is feasible from a materials viewpoint for both wartime and peace situations, and in most cases the polymeric encasement will probably outlive the usefulness of microchip.

Finally, the discussion in this section has also addressed some preliminary issues regarding the tag interface device section of the system. From the Army documentation received thus far by Battelle, it appears that this aspect of the system has seen the least amount of design development. Although several reader concepts exist, the manner in which these are to be connected to other systems, and the nature of applications software which resides in the tag interface device still needs a thorough design phase. Some of the issues which will impact this design are discussed in Chapter 6, "ADP System Compatibility".

7.1.3 Tag Interface Device (TID) Design Issue Summary

The nature of the TID functions make its design both critical and difficult. In particular, the host interface and data manipulation functions will be affected by all applications of the SDT system, either in its original

fielding or added later. Difficulties in making changes once the system has been fielded put extra emphasis on the need for flexibility, and on the importance of rigorous design review prior to implementation.

Specific TID hardware design issues, notably the tag interface and host interface, may be more significant economically and have a more global impact than currently thought. Firmware design is an issue which has received little attention to date but is capable of dominating the success of the system. Requirements for this function come more from interactions with host ADP systems than from the rest of the SDT system, and thus are not under control of the SDT system designers. Regarding security, the TID in general and its firmware in particular are likely points of attack. Design tradeoffs between software configurability and security may force an increase in TID complexity. The TID will probably require TEMPEST qualification, with the attendant requirements for shielding.

7.1.4 Cost/Benefit Analysis

There is a high potential for benefit from the SDT in both wartime and peacetime. The wartime benefits, although qualitative at this time, are very promising. Wartime benefits include higher return-to-duty rates, proper and quicker replacement of casualties, lives saved due to availability of medical records, alternative communications, and the creation/update of a theater-wide automated data system.

The peacetime benefits investigated are primarily the enhancements to the automated Army systems coming on-line. These enhancements include:

- Automatic retrieval of data files without keyboard intervention
- Accessibility of data when the automated system is unavailable
- Transportation of machine readable data to new locations in a more rugged medium than magnetic tape or disk.

The automatic retrieval feature utilizes the SDT as a means of identification. An SDT should provide correct retrieval every time. Currently identification must be verbally requested and keyed in for retrieval. Three

aspects of possible error in the current method are: incorrect identification supplied, incorrect understanding of identification data, and miss hit keys on the keyboard. SDT will bypass such errors.

Accessibility of data in austere areas is another advantage of the SDT. An SDT will be available even if an ADP system is unavailable. A soldier who is reassigned on the battlefield will carry his own file. The automated systems may not be able to be updated in real time during war. The SDT will allow local automated files to be created quickly, and in the event of computer destruction, will provide a mechanism to recreate files within the limits of the data in the tags. This aspect of SDT may be crucial for emergency medical in both wartime and peacetime. Army personnel entering facilities away from their station will have a backup file with them that will provide emergency information and enough identification to locate the automated file.

SDT may also be used as a unit's data carrier in both wartime and peacetime. Tactical and strategic plans may be carried on a tag when communication lines are tapped, cut, or jammed. A soldier caught wearing an SDT will not be an obvious carrier if all personnel are so equipped. During peacetime the tag will be used to carry data for reassignment. Clerk time will be cut for outprocessing and inprocessing by use of the SDT as a "traveling" data file.

Medical and personnel applications were recommended as a result of the CBA. Indications are that other beneficial applications may be and should be encouraged in order to increase the number of benefits as compared to cost. Examples of such applications are:

- As a meal card or proof of Basic Allowance for Subsistence
- As a loan record
- As a training record (attendance)
- As a jump record (attendance) or record of flight hours logged
- As a record of nuclear, biological, or chemical contamination.

Such applications would have minimal cost to add to an existing SDT with enough capacity and the benefits may be large.

A conclusion that is drawn from the use of multiple application is that a higher capacity tag is probably indicated. (Note that this is only the case if the additional applications cannot be supported by the data already carried on the tag. In some instances, particularly identification, the same data can be utilized.) A low capacity SDT may restrict the potential benefits that may eventually be realized.

In summary, the SDT will provide some wartime benefits, including saving lives, and will definitely have peacetime benefits (for medical/personnel application). Further, the SDT system will enhance the performance and usefulness of existing and planned ADP systems.

7.1.5 ADP Compatibility Issue

A major consideration with the Soldier Data Tag System is the need to interface with a variety of ADP systems. Within the Army this need is highlighted by the fact that most existing personnel, financial, and medical systems operate independently and on different hardware. However, the SDT concept is not restricted to the Army alone. Other service branches within DoD have data and processing requirements similar to those found in the Army. Because of the great potential for applying the SDT technology outside the Army, corresponding systems in the Navy, Air Force, and the Marines were studied from a compatibility viewpoint.

Throughout DoD many new systems are now being planned and developed and some old ones are being enhanced. In addition, new hardware is being procured to replace older terminals and computers. The need for the SDT to effectively interface with these systems is obvious. But, to be most effective, SDT specifications must be incorporated into the design of these systems.

7.2 General Recommendations

As noted in the Cost/Benefit Section of this study, in specific applications, the SDT appears to be cost-justifiable. These applications are characterized by the advantage of transferring the information with the

soldier instead of the current practices which involve use of procedures such as punched cards, potentially misrouted electronic messages, and manual data entry.

The successful implementation of the Soldier Data Tag system will involve the resolution of a number of detailed, technical design issues. These issues are discussed in detail in the Design Guide in this report. While these technical issues are important, it is Battelle's opinion that a number of strategic issues also need to be addressed. To that end, the following recommendations are presented.

Up to now, the SDT concept demonstrations have served to highlight the potential benefits of the system. While useful, these demonstrations have been small (both in numbers of soldiers and numbers of applications) and of too short a duration to gain the information necessary to develop a design specification for an Army-wide system. At this point, there is the need to gain operational experience and realize real productivity improvements in a limited environment.

The nature of this environment is that it must be large enough to adequately represent full-scale applications, while at the same time represent an application that can tolerate the problems that can arise in an evolving design. This step allows potential users of a full-scale system to become involved. These users include administrative personnel, ADP system designers, and the soldiers themselves. The results of this experiment would provide the field experience and information required for the full-scale implementation, including reliability and operability issues, as well as human factors requirements.

Attributes of a potential limited environment--or "showcase"--application include both the number of personnel involved, as well as the characteristics of the applications themselves. The following traits are desirable:

- **The tag-carrying population should be large**, perhaps between 10,000 and 30,000. This would permit an adequate test of manufacturing and distribution channels, as well as providing statistically significant usage and reliability data.
- **The showcase application should use a stand-alone SDT system.** This flexibility allows the system operation to be changed as necessary during testing, with no

effect or reliance on other ADP systems. Since the SDT will ultimately interface with other ADP systems in a full-scale implementation, the tag interface device (TID) can simulate the role of the host ADP system during the test. By not interacting with outside ADP systems, the design steps typically associated with interfaces, communications protocols, and data standards would be eliminated.

- **The existing SDT prototype design (as implemented for the concept demonstration) should be utilized to the maximum extent possible.** A short design review should be undertaken to identify any critical issues in the detailed hardware or software design that should be resolved prior to the test. This will minimize risk while proceeding as quickly as possible to the pilot implementation.
- **The selected application (or applications) should save money.** Although the potential for intangible benefits is very high, direct cost savings would be more effective in gaining support for a full-scale implementation.
- **The SDT concept should be a clear choice for the application when compared to competing technical approaches.** One of the technical arguments often encountered during the development of portable data carrier-type applications is whether it represents an advantage over on-line, centralized systems. In many cases, the correct selection is not straightforward, and proponents of both sides can argue a strong case for their own technology. In the pilot application for the SDT system, it is strongly desirable to select an application that cannot be addressed easily by on-line ADP approaches. For example, manifesting operations represent a logistical problem that is efficiently solved using the SDT approach. Also, an SDT meal card that can reduce the millions of dollars of fraud, waste, and abuse in the meal system is also an application that is most effectively solved using a portable data carrier.
- **The selected limited environment should be in an arena where the applications can evolve.** As more information is learned regarding the SDT system, new applications should be able to be overlaid onto the existing system architecture. The pilot application will begin the development of a "proving ground" for the new SDT concept. Ultimately, the merging of the SDT with ADP systems could be accomplished in this manner.

Based on Battelle's past experience in this area, the above general recommendations can maximize the probability of a smooth integration of portable data carriers into the information processing environment. The methodology insures the implementation of the system proceeds quickly, while allowing all key players in the system development an ability to drive the design of the final system.

7.3 Identification of Areas for Further Study

Throughout the course of the study, several issues were identified as being important to the overall development of the Soldier Data Tag System, but outside the scope of the current contract. As specified in the statement of work, these additional study areas are briefly described below.

7.3.1 Design Review of Prototype SDT Equipment

A detailed design review and reliability testing of the prototype equipment should precede any pilot application or Army-wide implementation of the SDT system. Although there is no commitment to use the prototype SDT system in the final implementation, it is likely that this equipment will be used in pilot applications, and the final SDT system implemented Army-wide will resemble the current equipment in many ways. A detailed design review would minimize the risk in both the proposed near-term pilot applications, as well as any subsequent Army-wide implementation.

As potential pilot applications could involve tens of thousands of soldiers--and subsequent Army-wide implementation rests so firmly on the success of these pilots--a design review at this time could be a modest and sensible investment. The need for such a review should not imply that the current designs are problematic; after many months of development, it is just often the case that the equipment developer is too close to the design to effectively evaluate it. As a result of Battelle's involvement with many such reviews, design refinements are often identified which result in improvements to system reliability, performance, and cost. As outlined below, the scope of such a SDT system design review prior to this first, critical pilot application should include the tags and the tag interface devices.

Review of the tag design would be conducted by physical tests of the tags themselves. While it is possible to quantify the physical properties and limitations of these devices, such an analysis is not necessary at this time. It is most useful to simply "screen" the design based on a set of pragmatic experiments and establish the likelihood of surviving in the intended environment. Survivability of the tag in the face of commonly expected hazards should be verified by loading the tags with test data patterns, subjecting them to the hazards, then determining whether they are still functional by examining the patterns. Some of the hazardous conditions to be examined include:

- Temperature cycling and temperature extremes
- Commonly encountered fluids
- Radiation (X-ray, radar, electromagnetic)
- Battlefield threats (shock, vibration, noise, directed energy weapons, ECM)
- Humidity extremes.

When possible, these tests should be conducted using the real-world environment. For example, expected survivability of the tag when exposed to common chemical solutions (i.e., laundry detergent, perspiration, fuels, solvents, insect repellent, cologne) can be tested by exposing them to the solution for an extended period and then attempting to read the tag data. Where a real world test is impractical, a simulation should be relied upon. Battelle has extensive laboratory facilities for conducting such tests.

The tag interface device will also be exposed to severe environments and rough handling. Both survivability screening and design analysis should be employed to verify mechanical integrity, maintainability, and operability. The interface device should be operated under temperature extremes and cycling, vibration, humidity variations, dusty environments, as well as other expected hazards. These tests, along with the design review, will identify any problems in both the electronic system as well as in the physical interface to the tag metallic contacts.

END

DTIC

8-86