NISTIR 4315

A Collection of Technical Studies Completed for the Computer-Aided Acquisition and Logistic Support (CALS) Program Fiscal Year 1988 Volume 1 of 3, Text, Security and Data Management

Roy S. Morgan
Editor

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards
and Technology
National Computer Systems Laboratory
Gaithersburg, MD 20899

April 1990

Issued March 1991

U.S. DEPARTMENT OF COMMERCE
Robert A. Mosbacher, Secretary
NATIONAL INSTITUTE OF STANDARDS
AND TECHNOLOGY
John W. Lyons, Director

NISTIR 4315

A Collection of Technical Studies Completed for the Computer-Aided Acquisition and Logistic Support (CALS) Program Fiscal Year 1988 Volume 1 of 3, Text, Security and Data Management

Roy S. Morgan
Editor

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards
and Technology
National Computer Systems Laboratory
Gaithersburg, MD 20899

April 1990

Issued March 1991

U.S. DEPARTMENT OF COMMERCE
Robert A. Mosbacher, Secretary
NATIONAL INSTITUTE OF STANDARDS
AND TECHNOLOGY
John W. Lyons, Director

Executive Summary

The overall objective of the Department of Defense Computer-aided Acquisition and Logistic Support (CALS) Program is to integrate the design, manufacturing, and logistic functions through the efficient application of computer technology. CALS is a program to apply existing and emerging communications and computer-aided technologies in DoD and industry to:

- Integrate and improve design, manufacturing, and logistic functions; thereby bridging existing "islands of automation."
- Actively influence the design process to produce weapon systems that are more reliable and easier to support and maintain.
- Shift from current paper-intensive weapon support processes to a highly automated mode of operation, based on a unified DoD interface with industry for exchange of logistic technical information in digital form.

The CALS program was established by the Deputy Secretary of Defense in September 1985 to implement the recommendations of a Joint Industry/DoD Task Force. Management is provided by a DoD Steering Group, the OSD CALS Office, and a lead organization in each Military Department and the Defense Logistics Agency. The DoD CALS Office has obtained the support of the National Institute of Standards and Technology in the selection and implementation of CALS standards. An Industry Steering Group has also been established to focus the work of key industrial associations and the defense contractor community in CALS implementation.

The CALS strategy provides a plan for phased implementation of CALS. Phase I will apply current computer technology in existing/emerging DoD and industry systems for key logistic and design applications. Phase II will involve broad-based DoD and industry system redesign to implement advanced technology across a wider range of applications during the early 1990's. DoD is currently developing core Phase I requirements. Demonstrations and prototypes will support Phase I implementation, while advanced technology R&D continues for Phase II.

Implementation of the CALS program will result in:

- o Design of more supportable weapon systems.
- o Increased productivity and reduced cost of weapon system acquisition and logistic support.
- o Improved timeliness and accuracy of logistic technical information.
- o Enhanced operational readiness of military forces.

During FY86 NIST recommended standards to OSD which would be applicable to the DoD environment.[1] These recommendations included CALS use of standards in the areas of product definition, graphics, text, and data management.

CALS support work in FY87 focussed on the following activities: Developing a CALS framework, Development Plan and Core Requirements package; providing technical support for standards development and implementation; and conducting workshops and meetings to promote dialogue with the Services, the Defense Logistic Agency, and industry. A major thrust was the completion of the initial documentation of the high-priority standards required for CALS implementation.[2]

During FY88, a number of efforts advanced the development of technology and standards in support of CALS. These efforts were organized into the areas of Text, Graphics, and Product Data.

Text: Work on text and graphics standards in the CALS publishing environment included technology assessments, development of application guidance, conformance test plans and a draft FIPS for ODA/ODIF. Additionally, a technology assessment and proposed conformance testing strategy were developed for page description languages.

Graphics: The CALS efforts in CGM were continued and included work in the graphics standards committees and the expansion and updating of the CALS CGM Application Profile. The Application Profile was developed into a draft military specification. The draft was carried through the needed review and comment process and was published as MIL-D-28003 in December 1988. In addition, work on Extended CGM, or CGEM for CALS application was initiated. Work in

---

[1]Kemmerer, S., Editor, "Final NBS Report for CALS, FY86," U.S. Department of Commerce, National Bureau of Standards, NBSIR 87-3566, May 1987.

[2]Kemmerer, S. Editor, "A Collection of Technical Studies Completed for the Computer-aided Acquisition and Logistic Support (CALS) Program, Fiscal Year 1987," U.S. Department of Commerce, National Bureau of Standards, NBSIR 88-3726, NBSIR 88-3727, NBSIR 88-3728, and NBSIR 88-3729, March 1988.

the area of raster graphics continued. A draft MILSPEC for raster was developed which was later published as MIL-R-28002. The need for standards for the interchange of large format tiled raster documents was identified, and related technical papers were published separately as an NIST Internal Report.[3]

Product Data: The use of the Information Resource Dictionary System, (IRDS, ANSI Standard X3.138-1988) was proposed as an integration and configuration management mechanism for the Product Data Exchange Specification (PDES).

---

[3]Spielman, F., Editor, "Standards for the Interchange of Large Format Tiled Raster Documents," U.S. Department of Commerce, National Bureau of Standards, NBSIR 88-4017, December 1988.

These three volumes are a collection of the final reports presented to the DoD CALS Office.[4] The collection is divided as follows:

VOLUME 1.

Text, Security, and Data Management

Text and Graphics Standards in the CALS Publishing Environment

ODA/ODIF Application Guidance

Federal Information Processing Standards Publication (Draft) on Document Application Profile for the Office Document Architecture (ODA) and Interchange Format Standard

ODA/ODIF Conformance Test Plan

PDLs: A Technology Assessment

SPDL Conformance Strategy

Security

Risk Management Tools: A Guide to Selection and Use

Computer Security Issues in the Application of New and Emerging Information Technologies

Data Management

Information Resource Dictionary System: An Integration Mechanism for Product Data Exchange Specification

Using the Information Resource Dictionary System for PDES

VOLUME 2:

Graphics, CGM MIL-SPEC

CGM Conformance Testing

Final Phase I.1 CGM MILSPEC

Extended CGM MILSPEC Planning

---

[4]The publishing of this collection of reports does not imply that the CALS Office has endorsed the conclusions or recommendations presented.

VOLUME 3:

Graphics, CGM Registration

CGM Registration in Support of CALS

The following additional publications were completed by NIST during FY87 under separate cover. They are available through NTIS.

CALS Workshop Proceedings: CALS EXPO '88 'Quality and Productivity Through Integration" A DoD/Industry NIST Conference 4-6 October 1988

MIL-HDBK-59, Military Handbook: Department of Defense Computer-aided Acquisition and Logistic Support (CALS) Program Implementation Guide

MIL-STD-1840A, Automated Interchange of Technical Information

MIL-D-28000, Military Specification: Digital Representation for Communication of Product Data: IGES Application Subsets

MIL-M-28001, Military Specification: Markup Requirements and Generic Style Specification for Electronic Printed Output and Exchange of Text

MIL-R-28002, Military Specification: Raster Graphics Representation in Binary Format, Requirements for

MIL-D-28003, Military Specification: Digital Representation for Communication of Illustration Data: CGM Application Profile

CONTRIBUTIONS

NIST would like to acknowledge the major technical contributors to this volume. In alphabetical order they are:

Dennis Gilbert

Irene Gilbert

Frances Nielsen

William Polk

Bruce Rosen

Lynn Rosenthal

Joan Tyler

Lawrence Welsch

TEXT

Text and Graphics Standards in the CALS Publishing Environment

CALS SOW TASK 2.1

TEXT and GRAPHICS STANDARDS in the CALS PUBLISHING ENVIRONMENT

ABSTRACT

The creation, distribution, and maintenance of technical publications is an expensive, time-consuming, and labor-intensive process. The process involves multiple people and organizations, as well as a variety of computer systems and applications. To reduce the growing costs and increase the efficiency in producing technical publications, emphasis is being placed on electronic or computer-aided publishing systems.

This report examines the role and rationale of text and graphic standards in the CALS publishing environment. It explores why standards are needed, the use of standards in the CALS environment, and how standards affect the document preparation and publishing processes. A model of the publishing processes with links to the standards is presented. Additionally, an evolutionary plan for implementing the model is presented, followed by recommendations and issues that need to be resolved.

Keywords: CCITT Group 4, CGM, electronic publishing, IGES, ODA/ODIF, Raster, SGML

Table of Contents

List of Figures

List of Tables

ACKNOWLEDGMENTS

The author would like to thank Judi Moline for the use of her compilation of information on standards, which appears in Appendix A of this report.

Disclaimer

The identification of commercial products or vendors does not imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the products identified are necessarily the best available.

I. Purpose

To examine the role and rationale of SGML, ODA/ODIF, PDL, CGM, Raster, and IGES in CALS and produce a paper for coordination and comment among the services and other organizations (SOW task 2.1, January 15, 1988).

II. Background

We need to improve today's publishing solutions, creating a seamless integrated environment. We need an environment in which information is electronically created, viewed, revised, stored, assembled, designed and disseminated among a variety of systems. The efficiencies of this achievement include savings in production time, cost, and labor. Specifically, we could eliminate the recreation of information, reuse previously created data, and disseminate information more efficiently.

Figure 1 presents a simplistic model of the CALS publishing environment. In general, it involves five subprocesses or steps:

1. Planning The contracting agency and contracting officer determine the content and visual specifications (MILSPECs) for the document.
2. Creation Contractor's authors and artists create original text and graphics.
3. Database Information is entered into the database in a structured format suitable for automated retrieval. Implementations of document databases are not yet widely available.
4. Composition Contractor's designer and compositor convert the text into typeset matter, scan graphics into digitized form or convert to film, and assemble into pages. The proofs are then reviewed for correctness by both DoD and the contracting personnel.
5. Presentation and Dissemination The document is printed on a specific device, bound and prepared for shipment. If the document was prepared from a database, the document can be composed for output to different devices, e.g., CD-ROM or CRT.

Until recently, the document production process was dominated by manual processes and paper. Regardless of how the information was created, paper copies were distributed for review or further processing. Each change required a new original to be generated. This method of document production does not easily allow for changes in content or design at any stage and precludes the reuse or continued processing of information.

Today's electronic publishing technologies have provided the tools necessary to eliminate many of the manual aspects of producing and publishing documents. However, current implementations still leave many of the manual processes in place. Because the processes are being automated independently, they are unable to efficiently communicate with one another. This creates islands of automation. The mode of operation, once again, is to resort to paper output and manual methods of document preparation and processing.

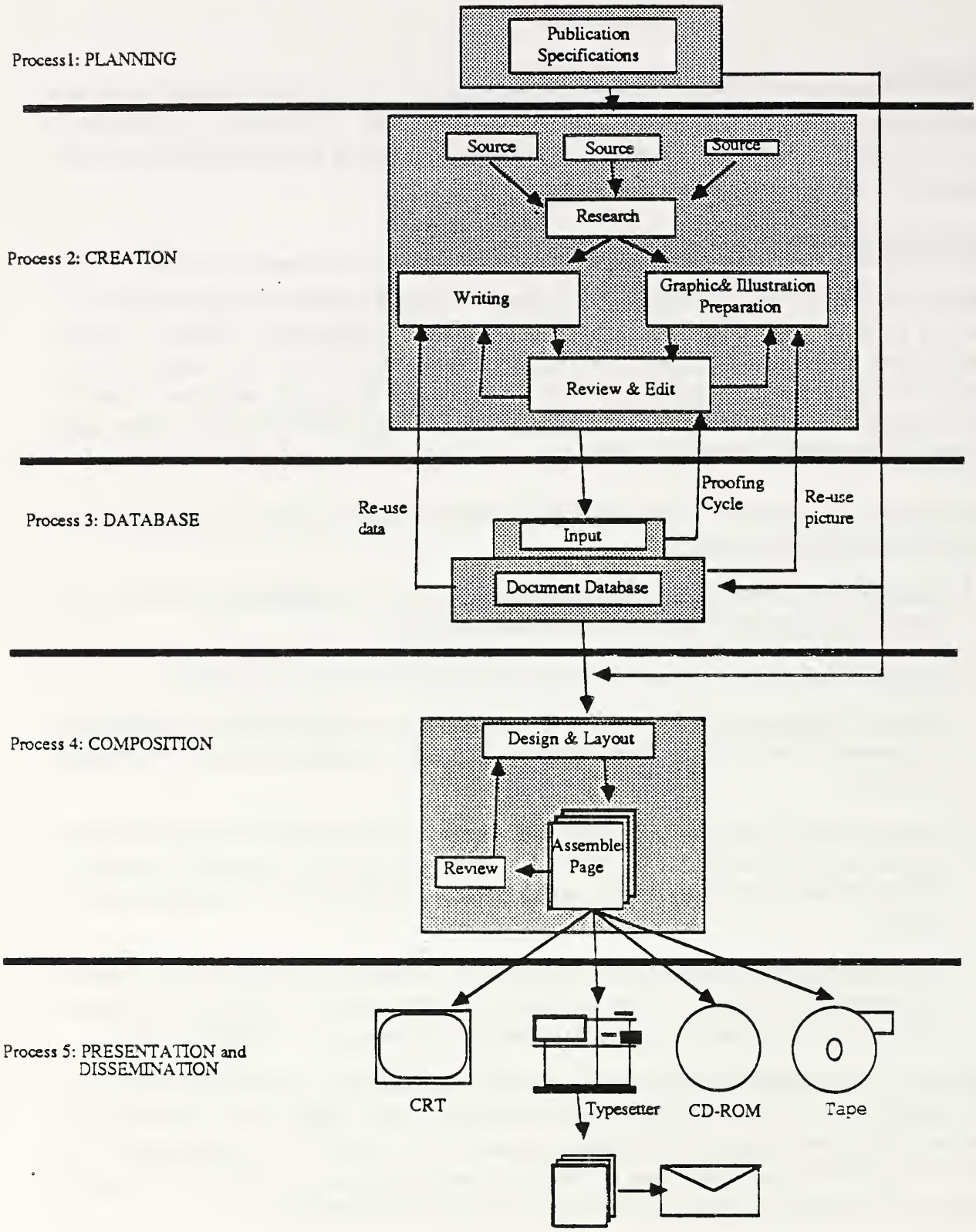


Figure 1: Publishing Work Flow Model

III. Discussion

The creation, distribution, and maintenance of technical publications is an expensive, time-consuming, and labor-intensive process. The process involves multiple people and organizations, as well as a variety of computer systems and applications. To reduce the growing costs and increase the efficiency in producing technical publications, emphasis is being placed on electronic or computer-aided publishing systems.

The goal is to improve DoD's ability to plan, publish, and distribute technical documents by expanding its capability to electronically create, transmit, use, and distribute technical information. In order to accomplish this goal, it must be possible to exchange and process information among dissimilar text, graphics, and publishing systems. However, the wide variety of representations for text and graphics created by the different technologies presents an obstacle to widespread exchange. There are hundreds of text formatters, graphics drawing packages, CADD systems, and scanner software, each with its own conventions for representing data, formatting instructions, and organizing the structural relationships among its components.

One solution to this undesirable heterogeneity is by providing information processing and interchange mechanisms that are independent of any system, device, application or data. Standards are such a mechanism. Using standards, information can be effectively shared among dissimilar systems and integrated together. Moreover, the quality and consistency of the information is assured. This report examines the role and rationale of text and graphics standards in the CALS publishing environment. It explores why standards are needed, the use of standards in the CALS environment, and how standards affect the document preparation and publishing processes. A model of the publishing processes with links to the standards is presented. Additionally, an evolutionary plan for implementing the model is presented, followed by recommendations and issues that need to be resolved.

IV. Role and Rational of Text and Graphics Standards

Figure 2 shows the technologies that are part of the CALS publishing environment. Text is created by different authors using different input devices. Graphics are developed on a variety of design or illustration workstations, or may be obtained from scanned images or photographs. When possible, translators or filters convert the text and graphics information to a file format understood by the composition application software. Otherwise, the information is regenerated and pasted into the document. Finally, the document is output to one or several different types of output devices.

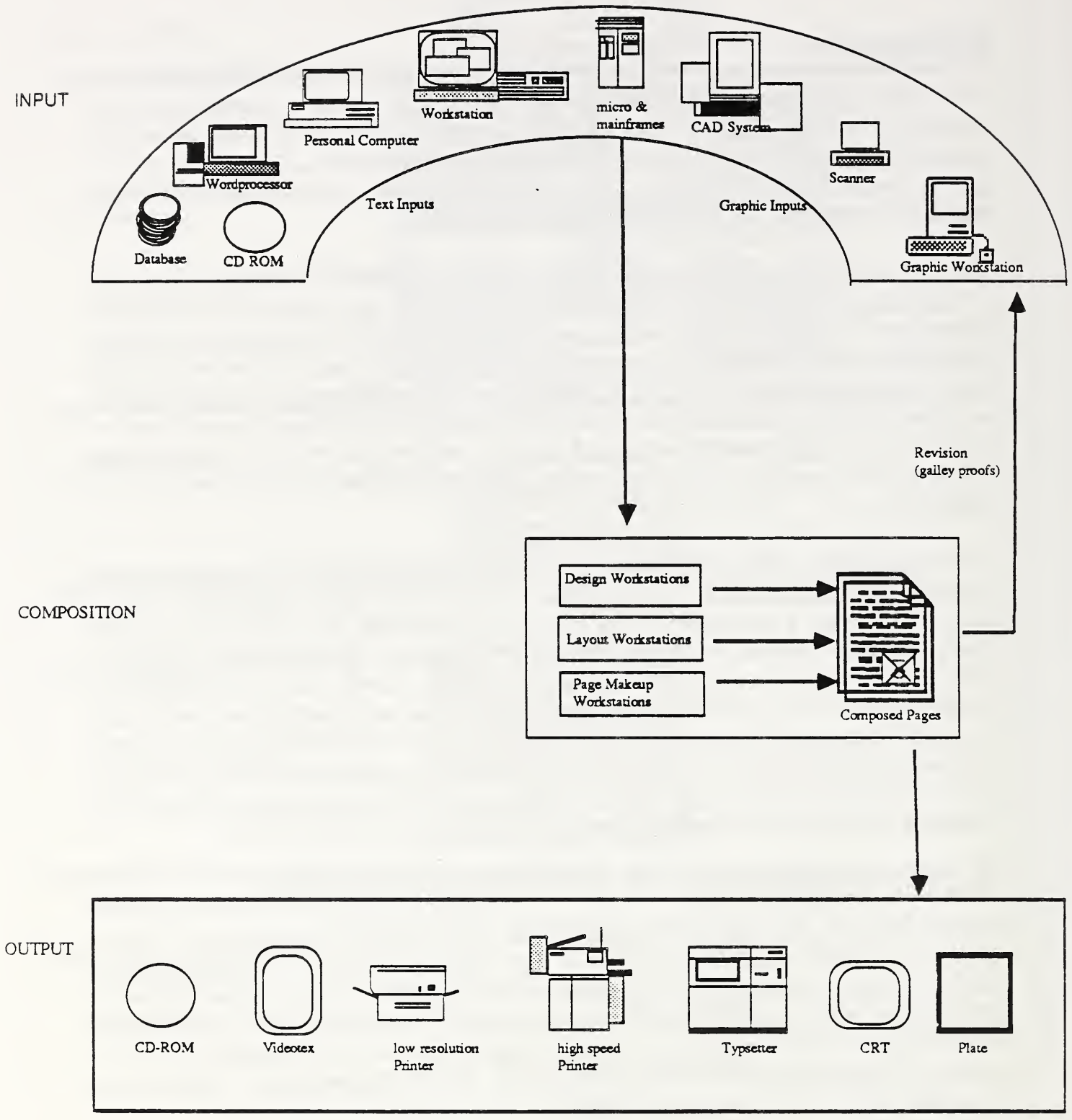


Figure 2: Publishing Process Technologies

A. CALS Needs

These requirements pertain to the development of a general publishing model for CALS documents. The publishing model must provide:

- physical connectivity among disparate systems with full communications including online communications and Email,
- support for data interchange standards,
- a structured database for the storage of text, graphic, and image elements of the document,
- configuration management and version control capabilities,
- multiuser access to a single document and sets of related documents with ability to change or revise,
- support for on-demand printing,
- the ability to reuse text, graphics, and images in different formats and/or different documents,
- WYSIWYG text authoring and graphic creation capability,
- the ability to electronically interchange and integrate text, graphics, and images from various systems,
- complex document composition tools and/or formatters, and
- the ability to input from and output to a variety of devices.

B. Why Standards are Necessary?

As stated earlier, the diversity of technologies in electronic publishing have introduced problems in exchanging and processing electronically created documents. The problem revolves around the different and incompatible data formats produced by the different technologies.

Currently, we deal with incompatible data formats by using converters or filters to translate the information into a form understood by the processing software. However, the existing media conversion systems are inadequate and uneconomical because:

1. the appropriate conversion software is not always available,
2. few if any conversion software packages can adequately cope with graphics,
3. the conversion process may cause some loss of data and format information,
4. conversion software may vary because of the lack of conformance tests to validate the conversion, and
5. several conversions may be necessary since each conversion is unique to a particular system.

Adherence to standards will improve interoperability by providing information interchange between the diverse computing environments and applications. Standards alleviate the problems of information and system incompatibilities by representing the information in a neutral format and/or establishing agreed upon methods of operation.

C. Use of Standards in CALS Environment

Several standards for document interchange of textual and graphical data have been identified in the Statement of Work (Table 1). Appendix A provides an summary of each standard, its scope, description, and use. Since each standard is designed to achieve different objectives and apply to a different set of applications, no one standard can handle all of CALS text and graphic requirements. The following section describes the advantages of using each standard by emphasizing what makes it unique from the other standards.

SGML	Standard Generalized Markup Language
ODA/ODIF	Ofice Document Architecture and Interchange Format
SPDL	Standard Page Description Language
IGES	Initial Graphics Exchange Speicfication
CGM	Computer Graphics Metafile
Raster	CCITT Recommendation T.6, Group 4 Facsimile

Table - 1 List of Standards

1. Standard Generalized Markup Language (SGML)

SGML specifies a method for describing the content and structural elements of an electronic document through descriptive markup and the document type definition, respectively.

Descriptive markup enables an author using his favorite word processor to identify or tag the semantic components of the document. The document or its parts can be edited and reused to create new or derivative documents. Since SGML documents use the ASCII character set, they are human readable and can be viewed or printed on a variety of devices.

The document type definition (DTD) provides a formal definition of the document via a precise machine-readable notation. This allows a computer to perform error checking on the document, e.g., check for missing, misplaced and invalidly tagged elements, thus ensuring that the document adheres to MILSPEC document structures and specifications.

Additionally, SGML works well for preparing document parts for storage and retrieval in databases. The design of the database can be expressed as a DTD, with the records and fields of data expressed by the tagged elements. Since SGML provides a means to define concisely each field of data and the interrelationships between the fields, specific information can be extracted from the database on demand. For example, the extract may consist of all plumbing information for a specific ship.

2. Office Document Architecture and Interchange Format (ODA/ODIF)

ODA is the only standard that supports both a logical and layout structure for compound documents. This method of representing the document promotes the concept of the paperless office. In particular, a document can be generated on one system and interchanged and reproduced in its original format or processed on another system.

The contents of an ODA document can be character text, geometric graphics or raster graphics information. Both the graphic architectures are based on existing international standards, CGM and CCITT Group 4 facsimile, respectively. Future extensions to ODA include the ability to handle audio for voice annotation.

ODA/ODIF was designed for use over networks, in particular OSI[1]. Consequently, it has become the canonical form of interchange within the worldwide community including OSI and TOP[2] committees as well as the European and Asian Workshops for Open Systems Group. Its ASN.1 binary encoding offers several advantages because the type-length-value (TLV) pattern can handle non-character data (e.g., pixels) that may be included in a document.

Any interchange of documents between different systems requires a conversion of format from the originator's format to the recipient's. Although ODA requires that documents be converted to its neutral format, the use of ODA/ODIF as the single intermediate format:

- reduces the amount of conversion software needed,
- eliminates the need to perform multiple conversions on the same document between all systems,
- handles text and graphics within the same document, and
- eliminates the loss of information through the use of Document Appliation Profiles (DAPS), which are agreed upon subsets of ODA [3].

3. Standardized Page Description Language (SPDL)

SPDL is a device-independent representation of final form documents that can be output to any display or printing device. It is capable of representing all content types, intermixed in any way, as well as black and white, multi-level monochrome, or full color documents. Thus

1 Open Systems Interconnection

2 Technical Office Protocols Organization

3 one such DAP is the NBS Document Application Profile as specified in the NBS Implementation Agreements

an organization can support a variety of output devices without having to reformat and repaginate the document for each printer or display. This makes SPDL a valuable component of on-demand printing.

Another aspect of SPDL that makes it applicable to on-demand printing applications is that an SPDL document can be stored and interchanged for presentation at a later time and/or at other locations. The document printing is distributed to the various sites that need the document. They in turn, print only the number of copies and/or sections of the document that are needed. This reduces the need to warehouse thousands of copies of a document and eliminates the problem of being "temporarily out of print."

4. Initial Graphics Exchange Specification (IGES)

IGES provides a data format for describing product design and manufacturing information which has been created and stored in a computer-readable form. IGES information is intended for human interpretation at the receiving site [20]

Since most of the design and contruction work of CALS support systems is by contractors, IGES provides the means to exchange and store drawings and specifications developed on the different vendor CAD systems. This ability will enhance the planning, operation, and maintenance of a support system by providing an on-line, readily accessable digital database of all the CAD drawing for a specific support system.

IGES can be used for simulations since it allows an object to be modeled in two or three dimensions as well as viewed from a variety of perspectives. Simulations can be used to check the size, reliability or maintainability of a support system or its parts. For example, a simulation of a plumbing support system as it would be installed could be used to determine if the system would fit properly in the allocated space, adversely affect other support systems, and be accessable when repairs are warranted.

5. Computer Graphics Metafile (CGM)

CGM represents a snapshot of the final picture a program has created. It also provides a file format suitable for the storage and retrieval of picture description information [20]. In contrast to IGES, CGM only contains information about the graphic and none of the non-geometric data descriptions as found in IGES.

The CGM picture is stored in a device and resolution-independent manner making it possible to preview the picture on low cost displays as well as print it on high resolution printers, plotters, and camera systems. A preview capability saves time and money by providing a means of examining the picture prior to output on either slow or expensive media.

A common use of CGM is to transfer the graphic information from the creating application program to an output device that is either too slow, remotely located, or currently busy. In this manner, CGM acts as a format for the spooling system providing a compact and efficient method of transferring the graphic over a network or directly to the output device [12].

The color capability of CGM provides a way to improve visual comprehension by emphasizing or differentiating different areas of a picture. For example, in business graphics, color may be used to emphasize different areas of a pie chart; or on a floor plan diagram of a ship, color may be used to differentiate between the electrical and plumbing systems.

CGM provides a link between different systems and applications. In particular, a CGM picture could be imported into another graphics package for additional enhancements or sent directly to a publishing system. CGM should be used within a compound document to describe the graphical information.[4]

Additionally, CGM can be used for archiving computer generated pictures. CGM pictures may be archived for as little as a few minutes (e.g., when previewing output from a batch program) or as long as several years (e.g., to be restored at a later time and/or place). The metafile contains the information necessary for successfully restoring the picture at a later time or on a different graphics device.

6. Raster: CCITT Group 4

CCITT Group 4 defines a widely accepted compression algorithm for the storage and transmission of raster images. Its high compression ratio results in reduced storage and transmission costs as well as improved throughput and response time.

The error checking in Group 4 ensures a high accuracy rate for transmission. The Group 4 protocol can be transmitted over public data networks such as packet-switched networks (e.g., MILNET) and integrated services digital networks (ISDN). Transmission over telephone lines requires the use of a modem.

Group 4 can handle various sized documents, compressing either the entire page or selected sections of a page. This feature allows Group 4 to be used as part of a compound document[5], compressing only the areas containing raster information. Additionally, large scale drawings can be compressed as a set of independent rectangular areas. This improves the decompression speed as well as the interactive response time for applications where only a portion of the image is used at a time (e.g., viewing a large drawing on a display).

Additional work related to raster and CCITT Group 4 is being conducted by the Tiling Task Group, a group of industry, user, and government representatives and the American National Standards Institute's X3V1 and X3H3.8 technical committees. X3V1 in response to the Tiling Task Group is defining a tiled raster interchange format (TRIF) to be used in conjuction with ODA/ODIF. TRIF will provide a "format that supports operation on a subset of an image without requiring other portions of the image to be accessed" [23]. X3H3.8, Imaging Application Programming Interface committee is developing a toolkit for handling imaging applications. The scope of this work is currently under development.

4 CGM defines the geometric graphics content architecture used by ODA/ODIF.

5 Group 4 defines the raster graphic content architecture used by ODA/ODIF

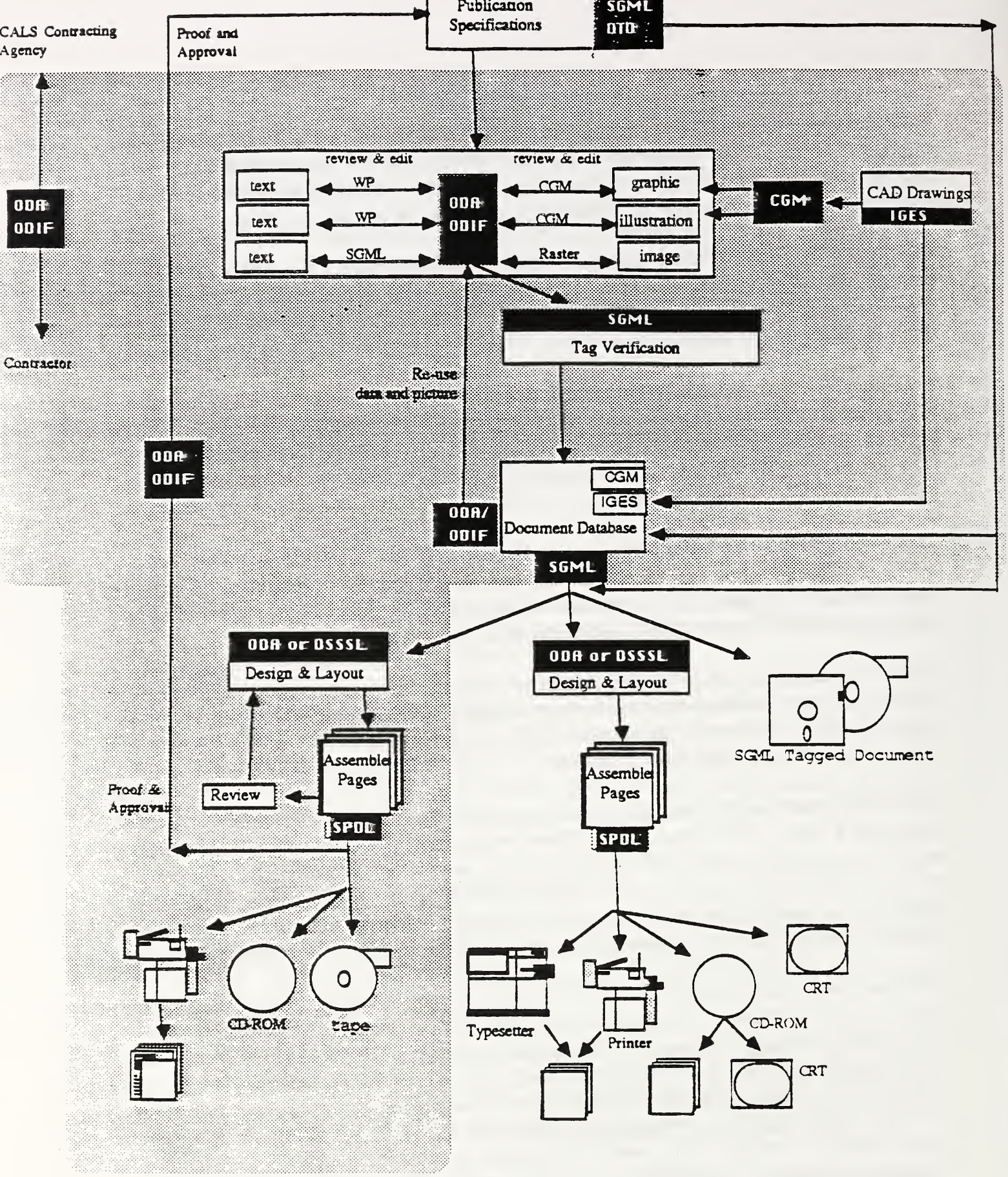


Figure 3: Publishing Model and Standards

V.CALS Publishing Model

A.. General Approach

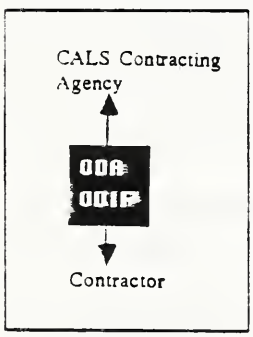
The model, Figure 3, is based on a structured database to represent the well defined, highly structured, often repetitive content and format of the technical publications. The database management architecture allows repetitive information to be recognized, shared, and reused. This approach eliminates data redundancy, reduces storage requirements, enhances data integrity, and improves configuration management and control [11].

Once information is stored in the database, all publishing activities are performed electronically. A document is generated by selecting the information constituting the parts of the document and automatically assembling the document according to specifications. The document can be output in its entirety or in part on a variety of devices including: printers, displays, videotext, CD-ROM, and magnetic tape.

B.. Description

The model shows the document preparation and publishing activities with links to the standards. The activities are to be performed by both the CALS contracting agency (CA) and the contractor. The shaded area of the model pertains to work done by the contractor. However, any activities in the shaded area could be performed by a DoD Publications and Printing Agency for producing in-house support documents such as training manuals and management reports.

CA-Contractor Communications: Contractor progress reports, memos, and other written communiques between the CA and contractor are interchanged electronically using ODA/ODIF. Unlike E-mail, telex, and the like, ODA/ODIF faithfully maintains the textual and graphical content as well as typefaces, formatting, and other typographical effects so closely allied with the content. Both the sender and recipient can be confident that the integrity and quality of the printed or screen representation of the document will be intact.



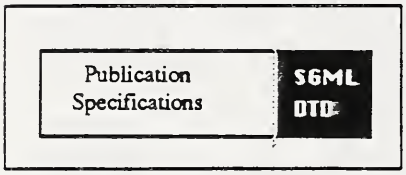
The reports are prepared on the document processing system of choice, converted to ODA/ODIF and electronically mailed. The received document is translated into the appropriate file format and ready to be viewed, edited, or printed.

The conversion software is provided with the document processor or acquired through a third party. The conversion software must implement the same ODA document application profile for this interchange to be successful. It is anticipated that vendors will implement the same core set of profiles, profiles that have been established by consensus and tested for

conformance. In particular, ODA/ODIF implementations should be based on the profiles defined by the NBS Document Application Profile (DAP) as specified in the NBS Implementation Agreements.

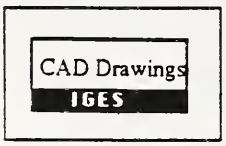
This step towards the paperless office provides for rapid document distribution, reduction in mail or messenger service costs, and ability to archive and maintain electronic record of transactions.

Publication Specifications: The CA provides the contractor with instructions and specifications for the digital and printed forms of the technical publication and required deliverables. The contractor must create and produce the technical publications according to MIL-STD-1840A MIL-M-28001, and MIL-M-38784B. The SGML markup tags, document type definitions (DTD), and output specifications as defined in MIL-M-28001 are used in:



- creating the SGML-tagged source file,
- structuring the document database,
- verifying document conformance, and
- outputing the document in the required format and structure.

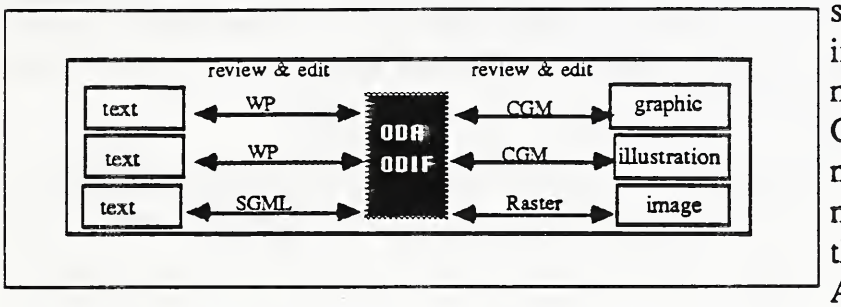
IGES: Designs created on CAD systems are stored in an IGES database. The CAD design can be included in the publication in either of two ways: first, as a 2-dimensional picture for inclusion in a publication or second, as a IGES file which accompanies the publication.



To include the design as a picture in the publication, IGES data is converted into a CGM file and transferred to a graphics workstation. This conversion is performed so that the graphics can be interchanged via ODA/ODIF and further edited if necessary. The CGM file can be created from either a 2-D view of the IGES data with the hidden lines removed or a screen plot of a 3-D window. Once in CGM format, the file can be reviewed, enhanced, and modified before incorporating the graphics in the final composed publication document.

An IGES file is included in a document by means of a reference in the document source file to a separate IGES file. To ensure correct document processing, the reference indicates the relationship between the document source file and the IGES file. Both the document and IGES databases are required and must be present in order to process the document. The final composed technical publication consists of a hardcopy or softcopy version of the publication and the IGES data as viewed on a CAD system or as a 2-D, static picture extracted from the database.

Creation: Authors and artists create the document using the workstation and application software of choice. Document inputs consist of original information, scanner input, and CAD pictures as well as information reused from the document database or received from the appropriate DoD entities. As the parts of the document are created, they are interchanged between authors, artists, editors, and reviewers for comment, revision, additions, restructuring, and finally, approval. This interchange is accomplished using ODA/ODIF formatted processable form. Each system provides a conversion to and from the formatted processable form.



For example: Information created by System A is converted to ODA/ODIF by Format Converter A and transmitted to System B. System B's Format Converter converts the ODA/ODIF file into system B format so it can be viewed, edited, printed, etc.

The exchanged information is reproduced in its original format by the receiving system, using the encoding techniques of the receiving system. Receiving documents with content and formatting preserved promotes the readability of the document parts and allows coauthors, artists, and reviewers to find and correct errors that relate to content as well as content-formatted errors, such as:

- mathematical formulas,
- alignment of data in columns or tables, and
- pictures and captions.

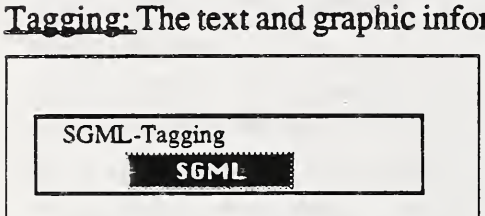
The ODA document profile can provide information related to the tracking, status, and version control of the document or its parts as well as the storage and retrieval of the document. Moreover, the profile indicates the level of conformance (that is, subset of ODA) adhered to in the document. This enables the recipient to determine which capabilities are required for processing or imaging the document. The document profile is interchanged along with the document or can be sent separately.

Networks provide the connectivity mechanisms to link the workstations and systems together. The functions provided by the network should include at least the following:

- the ability to share text or graphic files,
- the ability to control access to shared information,
- the ability to keep track of the status and version of each file, and
- E-mail.

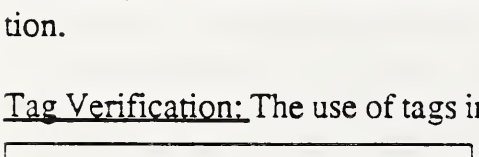
Other capabilities might include: remote execution, peripheral sharing, print spooling, wide-area network connections, log-on security, backup, network file management, and the ability to find a file stored somewhere on the network. These functions and capabilities may be provided as part of the network software, publishing software, add-on utility software, or by a combination of these software products.

Tagging: The text and graphic information is tagged in accordance with the specific application of the SGML, as specified in MIL-M-28001. The tags identify the document elements and the relationships of the elements (i.e., structure) to each other and the document as a whole. Additionally, the tags will be used in building the logical structure of the ODA/ODIF representation of the information (see Database section below). Proper tagging of elements is crucial to the verification of the document structure, storage of the document elements into the database, and retrieval and automated processing of the final document.

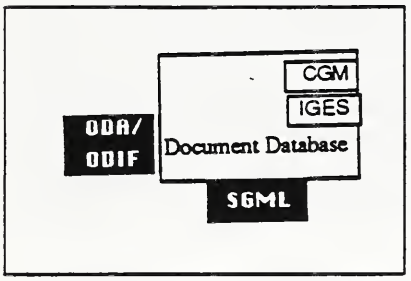


The information can be marked-up manually by the authors as they create the information, or by document analysts after the information is created, or can be generated automatically through software programs. These software programs may be part of the document processing or publishing software (e.g., Context SGML, Datalogic's Pager), bundled with the publishing software (e.g., Xerox Publishing System/InterMedia publishing configuration), or a separate utility (Officesmith's The Officesmith, Avalanche's IMSYS, Shaftstall's SGML Translator). Applying heuristic techniques, these software programs analyze the structural components of the document and apply the appropriate SGML tag(s). Raster and CGM graphic files are tagged so that they can be stored appropriately in the document database, referenced in the source document, and merged into the final composed publication.

Tag Verification: The use of tags in the preparation of the document are checked for invalid tags or misplaced elements and to ensure that all elements adhere to the parameters specified by the DTD. A parser, using a specific DTD, checks that the tags appearing in the input document conform to the DTD. Since the document will be created as fragments of the whole document (each author creates a fragment), the parser must be able to validate document fragments, not just the entire document. The parser finds and reports all markup errors. If errors are found, the document is returned for correction.



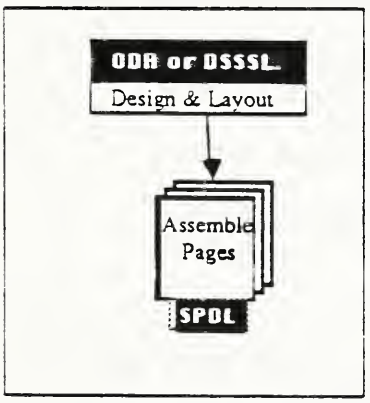
Database: The document parts are automatically loaded into the document database. The tags may or may not be retained in the database depending on the database software and design. However, if the tags are retained in the database, the application software must be able to distinguish between the tag and the element content. It must not misinterpret the tags as content or vice versa, and must know when to include or supress the tags. The DTD is the basis of the document database design. The database fields, field attributes, and interrelationships among fields are derived from the elements in the DTD. To achieve maximum benefit from the database, the data must be organized to reflect both current and future uses of the data.



On the output side, the data is either retrieved by the authors and artists for modification or reuse, or assembled automatically into an SGML-tagged source file plus graphic files. The data accessed by the authors/artists is sent with SGML tags through an ODA/ODIF processor which creates a formatted processable representation of the information. This ODA representation of the information is provided to the author/artist's system.

The SGML-tagged source file is validated as a conforming or nonconforming document by a parser. If a nonconforming document is unacceptable, it is returned to the author (via ODA/ODIF) for correction. Otherwise, the contractor inputs the SGML-tagged source file to the composition and output processors. Alternatively, the SGML-tagged source file and all relevant files (e.g. graphic files) are delivered to the contracting agency who proceeds to compose the final document.

Composition: The composition process consists of:



1. Translation: translating the markup and processing instructions into the text and graphic composition specifications needed to direct document composition.

2. Document composition: processing of the document including line composition, hyphenation and justification, processing of graphics information, and page makeup.

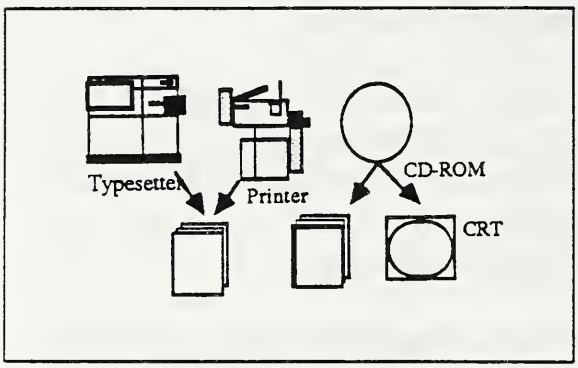
The automated composition processing functions to be performed on the SGML-tagged document are specified in Appendix C of MIL-M-28001. The format and style default values are set to conform to MIL-M-38784 or tailored to satisfy the contract requirements.

The document format and style specifications are expressed in the Document Style Semantics and Specification Language (DSSSL) or by ODA presentation styles. These specifications determine the format and layout characteristics of the document as it is composed. Since there may be several mappings of the SGML markup to the format and style specifications, the document can be formatted in different ways. However, only one mapping be-

tween the mapping and specifications is used at any given point in the document. This facility provides for the document to be composed in the format and style appropriate for the desired output medium (e.g., paper, display, CD-ROM, tape).

The result of the composition process is a text presentation metafile represented in SPDL. The SPDL document is created directly by the composition process, which formats the SGML documents using DSSSL, or indirectly by a translator, converting the ODA final form document to SPDL.

Presentation: The SPDL is used to store the final form document on output media such as CD-ROM or magnetic tape and/or to drive an output device such as a printer or display. The contractor provides both hard and soft copy versions of the SPDL document to the CA. The CA stores, prints, or views the document as appropriate.



The composed SPDL document consists of composed lines and graphic representations with each one assigned to a precise position on a page. The SPDL document is combined with printing instructions (e.g., number of copies to print) and sent to the presentation device for imaging on a visible medium such as paper or a display.

VI. Evolutionary Plan

The publishing model is implemented as a series of steps over the next few years. As the standards mature and standard's conforming products reach the marketplace, they are incorporated into the model. Table 2 shows the anticipated arrival of the standard's conforming products.

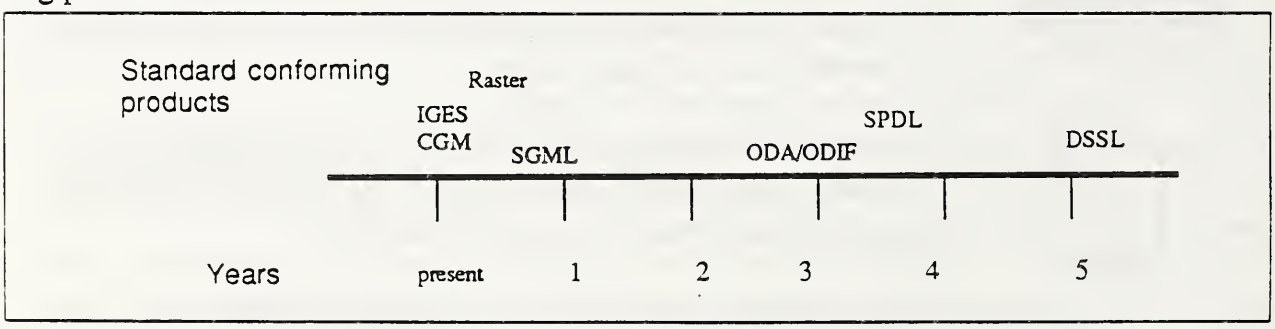


Table-2: Arrival of Standards Conforming Products

Sections A and B, below, provide a general summary of the availability of standards conforming products and a transition strategy for implementing the model over the next few years. Section C presents the technical and management issues that need to be considered to implement the model.

A.. Availability

IGES and CGM implementations are wide-spread, available from numerous vendors, and operate on a wide range of hardware platforms and operating systems. Translators to import and export IGES files on CAD systems, including micro-CAD systems and publishing software (e.g., Context, Interleaf, Datalogics) are readily available. Additionally, translators from IGES to CGM also exist, providing a bridge from IGES to CGM so that the image can be further processed by CGM systems.

Several vendors have begun to support the CALS Application Profiles for CGM. These profiles facilitates the interchange of graphics among diverse graphics devices. Although there is a high level of support by graphic vendors for CGM (e.g., Zenographics, Genigraphics, Computer Associates), other vendors are slower to follow. However, this is changing. There are several publishing packages, such as Lotus Manuscript, Aldus, Xerox Ventura, and Wang WP Plus, that can interpret and manipulate CGM files.

Raster or CCITT Group 4 compression and decompression algorithm for storing images is only available from a few vendors. However, the availability of compression chips from vendors such as AMD, Hitachi, and Ricoh will promote the acceptance of Group 4 among the vendors and will cause a steady increase in the number of available systems.

Although SGML authoring systems, parsers, and formatters are available, only a few adhere to MIL-M-28001. However, several vendors have announced their intent to produce CALS/SGML compliant authoring systems and document processing software. These systems include all or some of the following:

- auto-tagging software utilities which insert SGML markup into an existing document (e.g., ImSys by Avalanche),
- editors which enable authors to input tags as they create the document (e.g., Author/Editor by SoftQuad, SGML Writer by ArborText Inc.)
- parsers capable to fully supporting MIL-M-28001 (e.g., MarkIt by Sobemap),
- publishing software which parse and format the document (e.g., Context SGML by Context)

The availability of CALS/SGML systems will increase steadily as vendors strive to meet the CALS requirements.

For successful CALS/SGML implementation, there is a need for:

- the development of CALS/SGML document databases to incorporate the tagged document as well as software to retrieve the information from the database (e.g., hypertext),
- a method to backfit documents pre-dating CALS that are brought into the CALS environment,
- tools to assist document analysts in creating or modifying DTD's, and

- syntax-sensitive text entry tools to aid the author in following the document structure and using the tags correctly.

To date, there are no ODA/ODIF systems or convertors. However, efforts to implement ODA are underway and include:

- defining a set of document application profiles (i.e., functional standards for ODA) which, when implemented, will facilitate document interchange by minimizing the proliferation of profiles which implementors must implement and users must choose among,
- developing ODA toolkit which provides a set of subroutines for manipulating ODA documents, and
- developing pilot implementations to demonstrate the practicality and implementability of ODA.

B. Transition

To convert from the current publishing system to an electronic system as depicted in the model, current software and hardware may have to be modified or acquired to enable information to be electronically produced, accepted and stored. The software and hardware should evolve towards fourth wave integrated solutions[6], that is, systems that move away from proprietary hardware and software towards systems based on mainstream computing standards.

The objective of these systems is to promote distributed network publishing by providing an integrated publishing environment that:

- incorporates the desktop world into a larger system consisting of high-end systems and output devices,
- integrates text and graphic information,
- enables the free exchange of data between PC's technical workstations, CAD systems, and mainframe computers,
- provides transparent, distributed file access,
- provides document tracking, management and version control,
- includes tools for organizing, routing, and finding files,
- provides access to sophisticated composition, pagination and output capabilities through remote execution.

6 Fourth Wave is used to denote the fourth major change to the prepress industry. Wave 1 came with the introduction of hot-metal typesetting; Wave 2 came with the introduction of phototypesetting and production computers; Wave 3 came with the introduction of integrated computer-based systems; and Wave 4 is the shift from proprietary integrated systems to systems based on standards. Each wave of change redefines the publishing process and results in new vendors and product [25].

1. Current and Near Term Actions: (0-1.5 years)

Implementation of the model has already begun as demonstrated by MIL-M-28001, the required use of IGES systems for digital data exchanges among CAD systems, CALS Application Profiles for CGM, and the use of CD-ROM or magnetic tape to store documents for future viewing or printing.

All CAD and graphic systems should be capable of producing and accepting IGES and CGM files, respectively. Additionally, translators from IGES to CGM should also be put in place. Using software that can produce CGM output positions us for using ODA in the future.

Scanners are used to digitize hardcopy information. The image is compressed using CCITT Group 4 compression algorithms and stored in the document database.

To facilitate the document interchange between authors/artists, system integration tools such as translators, markup systems, file managers, and on-line communications are necessary. These tools should be based on existing standards wherever possible (e.g., SGML as the markup system, OSI for communications, and X.400 for electronic mail). Vendors who are committed to support the emerging text and graphic standards in future product releases should be targeted.

As CALS/SGML authoring, autotagging, and publishing systems develop, they should be implemented. A document database should be built to represent the relationships between the document elements and allow for the automated retrieval of information through its relationships. Meanwhile, document analysts must learn how to make modifications to the DTD when necessary, tag documents correctly, and backfit older applications.

Since there is no standardized output format (i.e., SPDL), the document should be composed for either a specific output device (as specified in the contract) or in several output formats (e.g., PostScript, HP's PCL, Interpress, and display oriented). Providing multiple formats promotes on-demand printing by maximizing the chances that the document can be output on the recipient's device.

2. Future Actions: (2-5 years)

All information is in digital form and is interchanged electronically.

Products that adhere to the standards continue to be implemented. As ODA and SPDL products become available they should be phased into the model, replacing the current proprietary based products.

At first, ODA implementations will consist of add-on conversion routines for existing products. It is anticipated that ODA/ODIF will be bundled with the application software and in some cases constitute the native file format produced by the software. SPDL will proceed in much the same manner.

Hypertext will be combined with electronic publishing to provide new interfaces for the management, access, storage and dissemination of information in the document database. With hypermedia, information is linked in non-linear ways, fact-to-fact rather than in a hierarchical arrangement (as in a book). Presented visually on a display screen, the hypermedia user can "travel" between linked frames of information, viewing and/or assembling the desired pieces of information. The hypermedia will automatically concatenate the contents of the frames, compose and paginate it according to a redefined document style and output the document in the SPDL format.

C. Issues to be Resolved

While developing the publishing model, a number of technical and management issues were raised. The following is a list of issues that should be addressed to ensure successful implementation of the publishing model.

1. Communications

A critical component of the publishing model is the communications infrastructure. Through network computing, the publishing processes and information can be distributed across a heterogeneous collection of computer systems. This improves personal and work group productivity by allowing users to collaborate through electronic file sharing and mail capabilities as well as distributing the work among the different publishing systems.

Purchasers of systems (i.e., the military) should address the following aspects of networking and its adminstration:

- network services: mail, messaging and conferencing, file service, remote task execution, print service, peripheral sharing
- network standards: OSI, GOSIP, X.400
- network types: PBX, PSDN, ISDN
- network operating systems: TCP/IP, NFS, RFS, Domain, 3Com, Appleshare, Tops, Novell

2. Other Standards

The development of fourth wave publishing systems is dependent on the use of standards. Standards other than the six addressed in this report may be relevant to the publishing process. These standards pertain to storage media (High Sierra Group Proposal), interchange formats (EDI, PDES), graphics (GKS, PHIGS), database (SQL), user interfaces (Windows), and operating systems (POSIX). Purchasers of systems should examine these and other potentially applicable standards to publishing and multimedia documents addressing:

- the role and rationale of the standard
- relationship to standards addressed in this report
- applicability to the CALS publishing environment

3. Conformance Testing

At present, there is a lack of testing procedures to validate a product's conformance to a standard. A set of tests are needed quickly to prevent the promulgation of products whose interpretation and implementation of the standards are considerably different and inhibit interchange. Conformance tests are used to identify problems, detect loss in functionality, and ensure correctness and completeness of the product. Developers of conformance tests should address at least the following:

- what should be tested and how
- recommendation for building a test suite
- procedures for using the test suite
- how errors shall be reported
- levels of conformance
- fidelity: handling of processing intructions and operating system dependencies
- certification procedures
- requirement for a certified testing laboratory

4. Barriers to Interchange

Because a product may have more capabilities than the standard provides, because the standard may not provide the same set of primitive descriptions of data as other systems, and because the standard may provide several ways to encode similar operations, interchange may not be successful [26].

To achieve true blind interchange between systems, both systems must implement in the same way either the entire standard or the same subset of the standard. Moreover, there must be an agreement as to conventions and assumptions made in translating documents between their native formats and the interchange formats described by the standards. Application Profiles, such as those developed for CGM and ODA should be used and developed to ensure the success of the interchange.

Although purchasers of systems should examine each standard as to its own implementation barriers, the following potential barriers should be examined for all standards:

- mapping between color and black and white
- specification and handling of fonts and font metrics
- maintaining text or graphic fidelity when mapping from the interchange format to the system's internal structure
- how rich an implementation a system can handle and how would a primitive system handle information produced by a richer system

5. Security

As systems are networked together and files are shared among users, security becomes an important issue. It must be possible to provide security and privacy of information on the systems. Purchasers of systems should address the following security requirements:

- authorization: establishing who may access which systems and information,
- access control: determining read-write-delete privileges for each file and user,
- file locking: preventing multiple users from editing the same file at the same time,
- backup and contingency planning: establishing procedures to ensure the availability of the systems, and
- data integrity: checking and assuring the correctness and accuracy of the information.

6. Proper Management

Proper management control must be exercised over the entire publishing process to ensure successful operation. The extent of this control and the following issues should be addressed by the system purchaser or implementor.

- software maintenance,
- configuration management and control,
- standards enforcement,
- motivation of users, and
- system expansion.

VII. Conclusions

The publishing model is designed to show the relationship of the publishing activities to the IGES, CGM, Raster, SGML, and ODA/ODIF standards. These standards work together, performing different but complementary functions within the model. Although they provide a fully functional, integrated publishing environment, the relevance of other text and graphic standards should be explored.

It should be recognized that this publishing model and related publishing technologies will lead to new ways of performing the basic functions within organizations. The potential for change should be nurtured and supported as long as it is consistent with organizational objectives and utilizes document and computing standards.

VIII. References

1. Arnold, D.B., and P.R. Bono. *CGM and CGI - Metafile and Interface Standards for Computer Graphics*. Springer-Verlag 1988.

2. ASME/ANSI Y14.26M-1987, *Digital Representation for Communication of Product Definition Data.*

3. Barkley, John. *Personal Computer Networks*. NBS Special Publication 500-140,

4. CCITT Recommendation T.5, *General Aspects of Group 4 Facsimile Apparatus*. 1984.

5. CCITT Recommendation T.6, *Facsimile Coding Schemes and Coding Control Functions for Group 4 Facsimile Apparatus*. 1984.

6. *CMU ODA Tool Kit, Application Programmers Interface*. Information Technology Institute, Carnegie Mellon University. January 1988.

7. Conversations with Joan E. Knoerdel. Aspen Systems.

8. Conversations with Fran H. Nielsen, National Institutes of Standards and Technology.

9. Gangemi, J. "SGML and Structured Database Design." *TAG The SGML Newsletter*. Volume 1, Issue 2, July/August 1987.

10. Grabowski, H. and R. Glatz. "IGES Model Comparison Systems: A Tool for Testing and Validating IGES Processors." *IEEE Computer Graphics & Applications*. November 1987.

11. Hansen, G. and J. Over. *Evaluation and Recommendations for Technology Insertion into Technical Order Maintenance*. Software Engineering Institute, Carnegie Mellon University. Technical Report CMU/SEI-88-TR-4, ESD-TR-88-005. May 1988.

12. Henderson, L., M. Journey, and C. Osland. "The Computer Graphics Metafile." *IEEE Computer Graphics & Applications*. August 1986.

13. ISO 8613: 1988 *Information Processing - Text and Office Systems -Office Document Architecture (ODA) and Interchange Format.*

14. ISO 8632:1986 *Computer Graphics Metafile for the Storage and Transfer of Picture Description Information (CGM).*

15. ISO 8879:1986 *Information Processing - Text and Office Systems - Standard Generalized Markup Language (SGML).*

16. ISO/IEC JTC 1/SC 18/WG 8 N561 *Information Processing - Text and Office Systems - Standard Page Description Lanaguage (SPDL).* 3rd Working Draft - 1988.

17. Knoerdel, Joan. "Databases: Knowing When, and How, to Use Them." *EP&P.* April, 1988.

18. MIL-STD-1840A: *Automated Interchange of Technical Information.* December 1987.

19. MIL-M-28001: *Markup Requirements and Generic Style Specification for Electronic Printed Output and Exchange of Text.* February 26, 1988.

20. National Computer Graphics Association. *Standards in the Computer Graphics Industry.* 1986.

21. NBSIR 88-3813. *Initial Graphics Exchange Specification, Version 4.0.*

22. Nuclear Research Center Karlsruhe, Department for Applied Systems Analysis and the Society for Mathematics and Data Processing Darmstadt. *Inpact Assessment on Electronic Publishing: Results of Phase II Report.* May 1988.

23. Polk, William T., *PDL's: A Technology Assessment,* Draft. NBS-Internal Report. June 1988.

24. Palmer, Mark E. *Strategies for Implementing IGES for the Operations of NAVFAC.* NBSIR 88-3693. January 1988.

25. "Publishing Joins the Mainstream." *The Seybold Report on Publishing Systems.* Volum 17, Number 9, January 31, 1988.

26. Sherman, Mark. *Translating Between ODA and Other Formats.* Information Technology Center, Carnegie Mellon University. May 1988.

27. TTG/88-14 *TRIF 2.0 Tiled Raster Graphics Content Architecture, proposed to ANSI X3V1 by the Tiling Task Group,* February 1988.

28. TTG/88-20 *Preliminary User Reqquirements for Tiled Raster Graphics TRIF 2.0,* March 11, 1988.

X. Appendix A: Summary of Text and Graphic Standards

The following summaries are extracted from NISTIR 88-3851, Document Interchange Standards: Description and Status of Major Document and Graphics Standards. September 1988.

STANDARD NAME: Standard Generalized Markup Language (SGML)

STANDARD NUMBER: ISO 8879

STATUS: International Standard (1986)

SCOPE: "This International Standard specifies an abstract syntax known as the Standard Generalized Markup Language (SGML). The language expresses the description of a document's structure and other attributes, as well as other information that makes the markup interpretable.

"This International Standard specifies a reference concrete syntax that binds the abstract syntax to specific characters and numeric values, and criteria for defining variant concrete syntaxes.

"This International Standard defines conforming documents in terms of their use of components of the language.

"This International Standard defines conforming systems in terms of their ability to process conforming documents and to recognize markup errors in them.

"Specifies how data not defined by this International Standard (such as images, graphics, or formatted text) can be included in a conforming document." (ISO 8879 "1 Scope")

DESCRIPTION: SGML was designed to interchange documents without regard to how the information was formatted. This allows for the use of the information in many different formats. SGML was designed to be application independent, and as such is very powerful when used in conjunction with a database application. The user is allowed to interact with and to modify the logical structures which are a primary part of his application. An SGML document may be processed by any formatter (for a formatting application) which has been suitably enabled with an SGML parser and other entity-management software. The SGML notation may be used to describe both logical and layout structures, if the format of the document is also to be interchanged. A set of standardized formatting semantics are to be provided by DSSSL. (Adler 2-3)

USE: SGML is specifically designed for the world of publishing and the management and control of the information which may take form in many types of documents.

"SGML can be used for publishing in its broadest definition, ranging from single medium conventional publishing to multi-media data base publishing. SGML can also be used in office document processing when the benefits of human readability and interchange with publishing systems are required." (ISO 8879 "0 Introduction")

REFERENCES:

Adler, Sharon C. "SGML and ODA: Two Standards for the Interchange of Documents," *<TAG> The SGML Newsletter*, Volume 1, Issue 4, 1-3.

ISO 8879:1986 *Information Processing - Text and Office Systems - Standard Generalized Markup Language (SGML)*, First Edition - 1986-10-15.

ISO 8879:1986(E) *Technical Errata* as of April 30, 1987.

Smith, Joan M. *The Standard Generalized Markup Language(SGML): Guidelines for Authors*. British National Bibliography Research Fund Report 27. Great Britain: The British Library, 1987.

STANDARD NAME: Office Document Architecture (ODA) and Interchange Format (ODIF)

STANDARD NUMBER: ISO 8613

STATUS: International Standard (1988)

SCOPE: "The purpose of this international standard is to facilitate the interchange of documents.

"In the context of ISO 8613, documents are considered to be items such as memoranda, letters, invoices, forms and reports, which may include pictures and tabular material. The content elements used in the documents may include graphic characters, geometric graphics elements, and raster graphics elements, all potentially within one document.

"NOTE : ISO 8613 is designed to allow for extensions, including typographical features, colour, spreadsheets and additional types of content such as sound." (ISO 8613-1:1988 (E) "1.1)

CURRENT WORK ITEMS:

Draft Addendum - Formal Specification of ODA Document Structures (FODA) (the Hague April 25-29, 1988)

DESCRIPTION: ODA was developed to allow the interchange of documents from one word processor to another. Page layout is handled according to some precise semantics which strive to be content independent. The page or sets of pages are specified denoting margins, columns, character path, line progression, etc., which detail the placement of rectangular "blocks," with content, specifically characters, image, and graphics to be poured in to occupy various areas on the page. (Adler)

The parts of the standard are as follows:

1. General Introduction
2. Document Structures
4. Document Profile
5. Office Document Interchange Format (ODIF) (see ODIF, ODL, and SDIF)
6. Character Graphics Content Architectures
7. Raster Graphics Content Architectures (see Raster and TRIF)
8. Geometric Graphics Content Architectures (see GGCA)

USE: ODA/ODIF is specifically designed for the interchange and replication of office documents in exact format. The design strives to be content-independent in order to allow for future content architectures such as audio information or possible mathematical and scientific equations.

REFERENCES:

Adler, Sharon C. "SGML and ODA: Two Standards for the Interchange of Documents," *<TAG> The SGML Newsletter*. Volume 1, Issue 4, 1-3.

Horak, Wolfgang. "Office Document Architecture and Office Document Interchange Formats: Current Status of International Standardization" *Computer* (October 1985), 50-60.

ISO 8613:1988 (E) *Information Processing - Text and Office Systems - Office Document Architecture (ODA) and Interchange Format*. March 1988.

STANDARD NAME: Office Document Interchange Format (ODIF)

STANDARD NUMBER: ISO 8613-5

STATUS: International Standard (1988)

SCOPE: "The purpose of this International Standard is to facilitate the interchange of documents.

"In the context of ISO 8613, documents are considered to be items such as memoranda, letters, invoices, forms and reports, which may include pictures and tabular material. The content elements used within the documents may include graphic characters, geometric graphics elements and raster graphics elements, all potentially within one document.

"ISO 8613 applies to the interchange of documents by means of data communication or the exchange of storage media." (ISO 8613-5 "1 Scope")

DESCRIPTION: "This part of ISO 8613:

— defines the format of the data stream used to interchange documents structured in accordance with ISO 8613-2;

— defines the representation of the constituents which may appear in an interchanged document. (ISO 8613-5 "1.3")

"ODIF is an abstract data syntax in which the constituents and attributes of the document are represented by a hierarchy of data structures and data items, specified using the abstract syntax notation ASN.1 defined in ISO 8824. "The coded representation of each data structure or data item is obtained by applying a set of encoding rules." (ISO 8613-5 "4.1 ODIF")

"The ODIF data stream is described in terms of a set of data structures, called 'interchange data element', which represent the constituents (document profile, object descriptions, object class descriptions, presentation styles, layout styles and content portion descriptions) of a document. The formats of the interchanged data element according to ODIF are defined using the Abstract Syntax Notation One (ASN.1) specified in ISO 8824." (ISO 8613-1 "6.4 Part 5 Office document architecture format (ODIF))"

USE: A document structured in accordance with ISO 8613 may be represented for interchange by the Office Document Interchange Format (ODIF). Since ODIF is a data structure specified using ASN.1, it is intended for use in an OSI environment. (ISO 8613-5 "4 Document representations")

REFERENCES:

ISO 8613-1:1988 *Information Processing - Text and Office Systems - Office Document Architecture (ODA) and Interchange Format*

ISO 8613-5:1988 *Information Processing - Text and Office Systems - Office Document Interchange Format (ODIF)*

STANDARD NAME: Standard Page Description Language (SPDL)

STANDARD NUMBER: ISO 3rd Working Draft. Feb. 19, 1988

STATUS: "Draft for Comment", Jan. 22, 1988

SCOPE: "The scope of this International Standard is the specification of a device-independent and process-independent description of images of documents in fully composed, non-revisable form. Such documents may utilize the full capabilities of imaging devices which may include high-resolution printing machinery and softcopy output devices.

"This International Standard is intended to be extensible in order to accommodate future developments in imaging technology.

"This International Standard is intended to be used in a variety of configurations meeting a variety of connectivity needs. It is specifically compatible with use over OSI networks."

"In addition to specifying how document images are represented, this International Standard specifies how additional information called *printing instructions* affects the document image. Printing instructions may be supplied with the request to print the document by means of a *print access protocol.*" (3rd Working Draft N561 "1.1 Scope")

DESCRIPTION: "The Standard Page Description Language is capable of representing all content types for fully composed, non-revisable documents. Any combination of the following types of content can be represented; any content may in [sic] black-and-white, gray-scale, or full colour; and content types may be intermixed in any way in the same document.

— character

— raster graphics

— geometric graphics."
(3rd Working Draft N561 "1.1 Scope")

USE: "This International Standard is intended for use in a wide variety of application environments, including:

— electronic publishing (including production publishing, workgroup publishing, desktop publishing, database publishing, electronic prepress, etc.)

— office systems

— information networks

— demand printing

"This International Standard provides a straightforward and efficient method of representing documents which are generated by ODA systems to presentation devices. It also provides a capability for similarly representing documents generated by SGML systems whose formatting is described by DSSSL.

"This International Standard allows for document presentation to be disjoint in both time and place from the document creation and formatting processes. It is specifically intended that SPDL document descriptions will be:

— sent directly to presentation systems which are accessed via a local connection

— sent to proximate or remote presentation systems via OSI or non-OSI networks, and

— stored or interchanged for the purpose of presentation at other times or at other locations."
(3rd Working Draft N561 "1.2 Field of Application")

REFERENCES:

ISO JTC 1/SC 18/WG 8 N561 *Information Processing - Text and Office Systems - Standard Page Description Language (SPDL)*, 3rd Working Draft - 1988-02-19.

STANDARD NAME: Initial Graphics Exchange Specification (IGES)

STANDARD NUMBER: American National Standard, ANSI Y14.26M - Digital Representation for Communication of Product Definition Data (same as IGES V3.0 specification)

STATUS: National Standard

SCOPE: "This Specification establishes information structures to be used for the digital representation and communication of product definition data. Use of this Specification permits the compatible exchange of product definition data used by various Computer-Aided Design and Computer-Aided Manufacturing (CAD/CAM) systems." (Initial Graphics Exchange Specification Version 4.0 June 13, 1988 "1.1 Purpose")

DESCRIPTION: "This Specification defines a file structure format, a language format, and the representation of geometric, topological, and non-geometric product definition data in these formats. Product definition data represented in these formats will be exchanged through a variety of physical media. The specific features and protocols for the communications media are the subject of other standards. The methodology for representing product definition data in this Specification is extensible and independent of the modeling methods used.

"Chapter 1 is general in nature and defines the overall purpose and objectives of this Specification. Chapter 2 defines the communications file structure and format. It explains the function of each of the sections of a file. The geometry data representation in Chapter 3 deals with two- and three-dimensional edge-vertex models, with simple surface representations and Constructive Solid Geometry (CSG) representations. Chapter 4 specifies non-geometric representations, including common drafting practices, data organization methods, and data definition methods.

"In Chapters 3 and 4, the product is described in terms of geometric and non-geometric information, with non-geometric information being divided into annotation, definition, and organization. The geometry category consists of elements such as points, curves, surfaces, and solids that model the product. The annotation category consists of those elements which are used to clarify or enhance the geometry, including dimensions, drafting notation and text. The definition category provides the ability to define specific properties or characteristics of individual or collections of data entities. The organization category identifies groupings of elements from geometric, annotation, or property data which are to be evaluated and manipulated as single items." (IGES Version 4.0 "1.2 Field of Application")

USE: IGES is used "to describe and communicate the essential engineering characteristics of physical objects as manufactured products. Such products are described in terms of their physical shape, dimensions, and information which further describes or explains the product. The processes which generate or utilize the product definition data typically include design, engineering analysis, production planning, fabrication, material handling, assembly, inspection, marketing, and field service." (IGES Version 4.0 "1.4 Concepts of Product Definition")

REFERENCE

ANSI Y14.26 M *Digital Representation of Product Definition Data.*

H. Grabowski and R. Glatz, "IGES Model Comparison System: A Tool for Testing and Validating IGES Processors," *IEEE Computer Graphics and Applications*, (November 1987) 47-57.

IGES V4.0 *Initial Graphics Exchange Specification*, Version 4.0, June 13, 1988.

IGES *Technical Illustrations Application Guide*, April 1987.

IGES *Recommended Practices Guide*, November 1987.

IGES *Electrical Application Guide*, March 1987.

MIL-D-28000 *Digital Representation for Communication of Product Data: IGES Application Subsets*, 22 December 1987.

MIL-STD-1840A *Automated Interchange of Technical Information*, 22 December 1987.

NBSIR 86-3359 *Initial Graphics Exchange Specification, Version 3.0.*

STANDARD NAME: Computer Graphics Metafile for the Storage and Transfer of Picture Description Information (CGM)

STANDARD NUMBER: ISO 8632

STATUS: International Standard (1986)

SCOPE: "The Computer Graphics Metafile provides a file format suitable for the storage and retrieval of picture description information. The file format consists of an ordered set of elements that can be used to describe pictures in a way that is compatible between systems of different architectures and devices of differing capabilities and design.

"The elements specified provide for the representation of a wide range of pictures on a wide range of graphical devices. The elements are split into groups that delimit major structures (metafiles and pictures), that specify the representations used within the metafile, that control the display of the picture, that perform basic drawing actions, that control the attributes of the basic drawing actions and that provide access to non-standard device capabilities.

"The Metafile is defined in such a way that, in addition to sequential access to the whole metafile, random access to individual pictures is well-defined; whether this is available in any system that uses this Standard depends on the medium, the encoding and the implementation.

"In addition to a Functional Specification, three standard encodings of the metafile syntax are specified. These encodings address the needs of applications that require minimum metafile size, minimum effort to generate and interpret, and maximum flexibility for a human reader or editor of the metafile." (ISO 8632-1:1986 1 "Scope and Field of Application")

DESCRIPTION: "The Computer Graphics Metafile provides a file format suitable for the storage and retrieval of picture information. The file format consists of a set of elements that can be used to describe pictures in a way that is compatible between systems of different architectures and devices of differing capabilities and design." (ISO 8632)1:1986 0.1 Purpose)

"The main reasons for producing a standard computer graphics metafile are:
a) to allow picture information to be stored in an organized way on a graphical software system;
b) to facilitate transfer of picture information between different graphical software systems;
c) to enable picture information to be transferred between graphical devices;
d) to enable picture information to be transferred between different computer graphics installations."

The parts of the standard are as follows:

1. Functional Specifications
2. Character and Coding
3. Binding and Coding
4. Clear Text Encoding

USE: "The use of this standard is strongly recommended when one or more of the following situations exist:

— A graphics metafile is maintained at a central facility for a decentralized system that employs graphics devices of different makes and models that must utilize the data.

— A graphics metafile is required to preserve picture data when conversion or migration from one graphics system to another is necessary and the two systems are not necessarily compatible.

— A graphics metafile is intended for information interchange between a source system and a target system that are not necessarily compatible."
(FIPS PUB 128 - Computer Graphics Metafile "9. Applicability")

REFERENCES:

Arnold, D.B. and P.R. Bono. *CGM and CGI: Metafile and Interface Standards for Computer Graphics.* Berlin: Springer-Verlag, 1988.

Henderson, Lofton, Margaret Journey, and Chris Osland. "The Computer Graphics Metafile." *IEEE Computer Graphics and Applications.* (August 1986) 6:8, 24-32.

ISO 8632-1986 *Information Processing Systems - Computer Graphics Metafile for the Storage and Transfer of Picture Description Information.*

NBS FIPS PUB 128 *Computer Graphics Metafile (CGM)* 1987 March 16.

STANDARD NAME: CCITT Group 4 Facsimile

STANDARD NUMBER: CCITT Recommendation T.5 and T.6

STATUS: International Standard 1984

SCOPE: The Group 4 Facsimile Standard has two parts. Recommendation T.5 "defines the general aspects of Group 4 facsimile apparatus. The Group 4 facsimile coding scheme and facsimile control functions are defined in Recommendation T.6." (CCITT *Red Book* Recommendation T.5 "2 Scope")

DESCRIPTION: "The Group 4 apparatus provides the means for direct document transmission from any subscriber to any other subscriber.

"All apparatus participating in the international Group 4 facsimile service has to be compatible with each other at the basic level defined in this Recommendation. Additional operational functions may be invoked.

"The range of data rates is described in Section 6. Detailed arrangements on a national level are left to the Administrations concerned, as it is recognized that national implementation of the Group 4 facsimile service on various types of networks may involve national operation at different data throughput rates.

"The page is the basis for facsimile message formatting and transmission. Both A4 and North American paper formats are taken into account.

"Facsimile coding schemes are applied in order to reduce the redundant information in facsimile signals prior to transmission.

"The apparatus must have the ability to reproduce facsimile messages. The content, layout and format of facsimile messages must be identical at the transmitting and receiving apparatus.

"The reproducible area is defined within which facsimile messages are assured to be reproduced.

"The Group 4 facsimile apparatus should provide means for automatic reception. In addition Class II/III apparatus should provide means for automatic reception of Teletex and mixed mode documents.

"All Classes of Group 4 facsimile apparatus shall incorporate the functions defined as basic for the Group 4 facsimile service in Section 3.2 below. In addition, optional functions can be incorporated. In this Recommendation, the optional functions are divided into CCITT standardized options and nationally and/or privately specified options." (CCITT *Red Book* Recommendation T.5 "3.1 Basic Characteristics")

USE: "Group 4 facsimile is used mainly on public data networks (PDN) including circuit-switched, packet-switched, and the integrated services digital network (ISDN). The apparatus may also be used on the public switched telephone network (PSTN) where an appropriate modulation process will be utilized.

"The procedures used with Group 4 facsimile apparatus enable it to transmit and reproduce image coded information essentially without transmission errors.

"Group 4 facsimile apparatus has the means for reducing the redundant information in facsimile signals prior to transmission.

"The basic image type of the Group 4 facsimile apparatus is black and white. Other image types, e.g. grey scale image or colour image, are for further study.

"There are three classes of Group 4 facsimile terminals:

— Class I - Minimum requirement is a terminal able to send and receive documents containing facsimile encoded information.

— Class II - Minimum requirement is a terminal able to transmit documents which are facsimile encoded. In addition, the terminal must be capable of receiving documents which are facsimile coded, Teletex coded, and also mixed-mode documents.

— Class III - Minimum requirement is a terminal which is capable of generating, transmitting and receiving facsimile coded documents, Teletex coded documents, and mixed-mode documents."
(CCITT *Red Book* Recommendation T.5 "1 General")

"Group 4 facsimile apparatus shall be capable of handling:

a. the basic end-to-end control procedures as defined in Recommendation T.62;

b. document interchange protocol as defined in Recommendation T.73;

c. the basic facsimile coding scheme as defined in Recommendation T.6;

d. the control functions associated with the basic facsimile coding scheme as defined in Recommendation T.6.

"All classes of Group 4 apparatus shall have the following provisions for facsimile messages:

a. provision for scanning the documents to be transmitted;

b. provision for receiving and presenting hard or soft copies of the documents.

"In addition Group 4 Class II apparatus shall have provision for receiving and displaying basic Teletex and mixed mode documents.

"In addition to the requirements for Group 4 Class II apparatus, Class III apparatus shall have provisions for generating and transmitting basic Teletex and mixed mode documents.

"Basic page formatting functions are as follows:

a. vertical page orientation;

b. paper size of ISO A4;

c. reproducible area/printable area is defined taking into account ISO A4 and North American paper formats and ISO standard 3535."
(CCITT *Red Book* Recommendation T.5 "3.2 Basic Functions")

REFERENCES:

CCITT *Red Book Vol VII fascicle VII.3 Terminal Equipment and Protocols for Telematic Services*. Geneva 1985.

TEXT

ODA/ODIF Application Guidance

CALS SOW TASK 2.2.1

ODA/ODIF APPLICATION GUIDANCE

I. PURPOSE

To produce an ODA/ODIF application guidance document suitable for inclusion in the CALS Implementation Handbook. (Task 2.2.1)

II. BACKGROUND

The growing use of personal computers for text processing and desktop publishing has highlighted the need for document interchange standards. Over the past several years there has been an effort to develop a standard for document interchange. As a result, the Office Document Architecture (ODA) and Interchange Format standard became an International Standard (ISO 8613) in 1988. It is also expected to be ratified by the CCITT at their November 1988 Plenary as a series of Recommendations (T.410).

The use of ODA allows for the interchange of documents containing character text, raster (facsimile) data, and computer generated images in one integrated datastream. It is believed that there exists a DOD need to interchange such compound documents, produced on various text processing systems, among other dissimilar systems.

III. DISCUSSION

The ODA/ODIF application guidance document has been produced as a result of NIST's participation in the development of the ODA standard and as a result of our leading role in specifying an Implementors Agreement for ODA. This Agreement, called a Document Application Profile (DAP), provides for the interchange of documents created by a range of text processing systems -- from the relatively simple WYSIWYG ("what you see is what you get") machines to the more sophisticated desktop publishing systems on the market today.

ODA document interchange is independent of the communications technology used to move the document; however, one important concept adhered to during the development of ODA was that of "open interchange."

Finally, ODA documents can be transferred in many forms. In particular, ODA documents may take the following forms: formatted (or final form) or processable (revisable, editable), or both.

NIST believes that the use of ODA for document interchange is a key ingredient in the CALS program.

IV. RECOMMENDATION

NIST recommends that CALS include the attached appendix to the CALS Implementation Handbook.

APPENDIX ____

APPLICATION GUIDANCE FOR ACQUISITION OF DIGITAL INTERCHANGE OF DOCUMENTS

1. SCOPE

The recent growth in the use of personal computers and decentralized computing allows users to create a wide range of documents containing text (character data), images, computer graphics and data. This has emphasized the need to be able to transfer information electronically both within, between and among various systems.

Another vital need is the ability to transfer processable documents; that is, documents which can be revised, edited, and/or further processed. For example, if multiple contractors are working together to produce an integrated technical report, it is essential that they can interchange documents among themselves, revise these documents as necessary, and continue their interactions.

Finally, there is a need to incorporate, within a single document, multiple types of content, such as character, raster data, and computer graphics.

This Appendix addresses the selection of a document architecture and interchange format to provide for digital interchange of processable technical manuals. Other uses for a document architecture and interchange format, not described in this appendix include the interchange of documents such as memos, letters, orders, informal reports, and technical reports.

Electronic document interchange offers numerous opportunities for improved efficiency and ease of use, for example, in the preparation of such documents and in their delivery, storage, distribution, and maintenance.

2. DECISION NODE DISCUSSION

Figure 1 shows the Decision Template for Digital Delivery of Documents. The alternatives contained in the decision template are described in the following paragraphs.

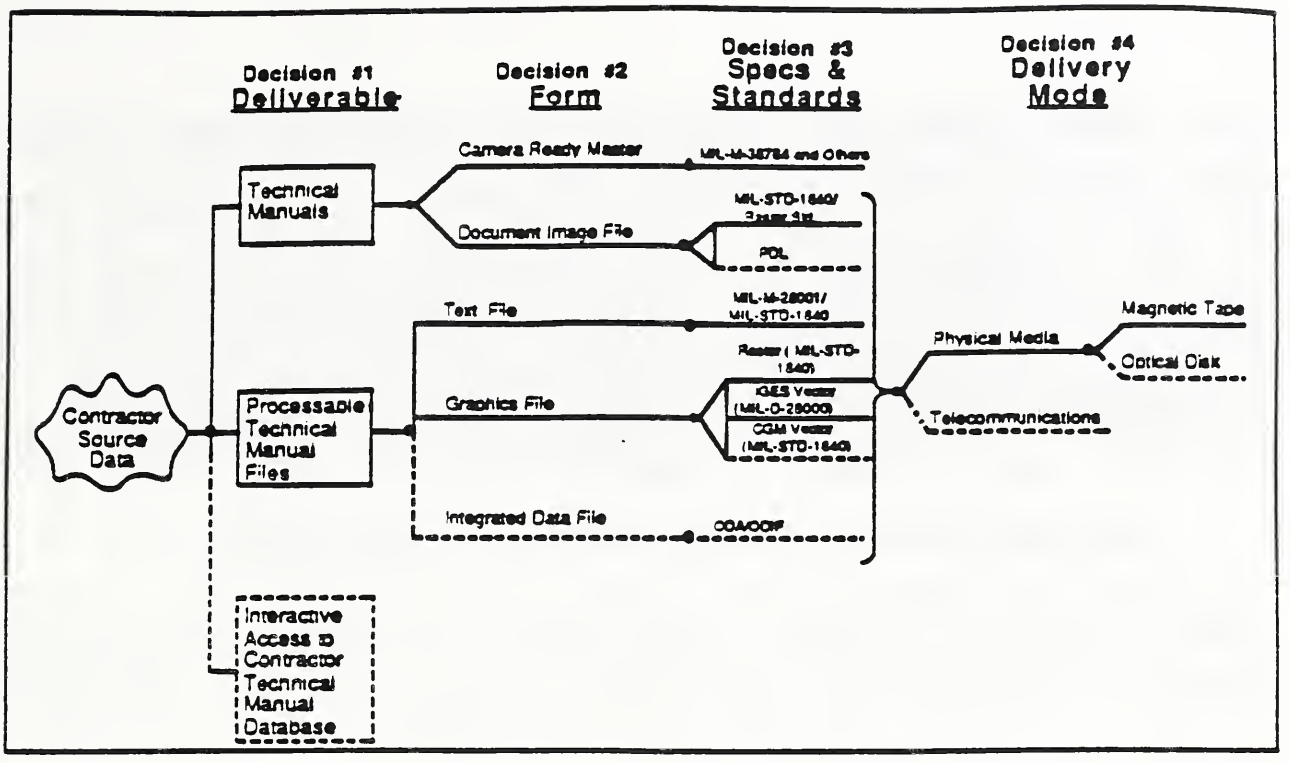


Figure 1. Decision Template

2.1 DELIVERABLE OPTIONS - DECISION #1

Documents may be delivered as final hardcopy (e.g., paper) or as digital data. Additionally the digital form of a document may be final (e.g., ready to be printed/displayed or archived) or processable (e.g., ready to be revised or edited) or both (i.e., includes information to print as final or to further process). Processable form documents offer the most flexibility and the least overhead of these. Processable files can be modified with ease. Until recently, however, it was unwieldy to process (e.g., modify) manuals containing both text and graphics since few systems handled integrated text and graphics. With the emergence of the document architecture and interchange format standard, this obstacle can be overcome. Digital data representing integrated, processable documents can be delivered as well as hardcopy.

It may be necessary to accept for each deliverable, both a hardcopy or printed document, for approval and a digital form of the document. It is expected that print-on-demand publishing systems may alleviate some of the need for hard copy deliverables.

2.2 FORM OPTIONS - DECISION #2

As shown in the figure, the forms for delivery of the final or non-processable document can be either a camera ready master (hardcopy) or a document image file (digital). The digital form consists of composed page images of the document. This form may be more efficient to view, distribute, store, and print than camera ready copy. Additionally, the digital form, though containing a rigid digital format, provides more flexibility

than camera ready copy which can only be manipulated by hand.

The choice of forms for delivering the processable document are to deliver each component of the document separately or to deliver an integrated data file containing text and graphics. At present, a processable file usually contains one set of files for text and separate files for graphics, such as illustrations and drawings. Now that there is a document architecture and interchange format standard which provides for integrated documents, this form of delivery should take precedence, wherever possible, over delivery of separate files.

2.3 SPECIFICATION/STANDARDS OPTIONS - DECISION #3

Page image documents may be either camera ready masters or raster scanned images. Raster images offer advantages of electronic storage, retrieval, display, and print-on-demand. Integrated digital documents offer the most advantages.

Digital delivery of both final form and processable form documents can be achieved by the use of the Office Document Architecture (ODA) and Interchange Format standard. ODA allows for the integration of text and graphics into one digital datastream and provides for final copy or processable data. Final form documents include layout structure which relates to the presentation of the document. Processable form documents include logical structure and support update and maintenance. ODA also provides for a combination of final and processable form. There are advantages to using one standard to provide for either or both forms of delivery. ODA should be incorporated into the CALS Implementation during Phase I.

A standard Page Description Language (PDL) provides for independent device drivers to output the final form documents. A standard PDL is expected during Phase I of CALS Implementation.

Camera ready masters should be delivered in accordance with MIL-M-38784 or other appropriate MILSPECs or MILSTDs. Digital page image files should be delivered in accordance with MIL-STD-1840.

Technical manuals acquired as processable files generally will contain both text and graphics. Graphics files may be in either raster or vector formats. Vector formats are easily edited, maintained, and updated; raster formats are more difficult to edit. Each of these graphics formats and text files or a combination of text and graphics formats may be delivered.

With respect to text, MIL-M-28001 (SGML) is the recommended specification. For raster graphics, a specification is being developed based on CCITT Group 4 facsimile. For vector graphics, two standards are available: MIL-D-28000 (IGES) and the Computer Generated Metafile (CGM) as discussed in Section 6.4.1.1 of MIL-STD-1840. Generally CGM deals with graphics such as figures, illustrations, charts, and so on, while IGES handles engineering

drawings. CGM files are smaller than the equivalent IGES files by a factor of up to four. CGM is the recommended option, but IGES is allowed.

For documents containing a combination of text, raster, and vector graphics, ODA should be used. Currently, ODA standardizes these three content types. The text portion of ODA allows for any registered character sets, the raster graphics portion caters for CCITT Group 4 facsimile, and the vector graphics (called geometric graphics in ODA) is CGM.

2.4 DELIVERY MODE OPTIONS - DECISION #4

Currently, the most practical option for delivery of digital documents is via physical media (e.g., tapes, diskettes). The size of the files to be delivered make it impractical and expensive to rely on telecommunications. For example, transfer of large raster image files is very costly.

The preferred physical media option is magnetic tape. Appendix III-A of this Implementation Guide list the tape media standards to be used. As optical disk and CD-ROM become more readily available and inexpensive, these may be suitable alternatives to magnetic tape. Optical disk and CD-ROM will be useful for archiving and database applications. Of course, these media will involve investment by both the contractor and the Government for processing.

2.5 SUMMARY

To summarize, the evaluation and selection of the options at each choice in the decision template should be responsive to the needs and goals of the military organization requiring the digital delivery of documents. Document image files should be acquired early in the life cycle of the program; processable documents should be acquired when the Government is responsible for maintaining, updating, and/or further processing the documents. The currently preferred option for the physical media containing such digital documents is magnetic tape.

3. DECISION GUIDELINES

The options given above are not necessarily mutually exclusive. That is, there may be a need to combine several options for specific deliverables or there may be a need to provide multiple selections of options. The Implementation Guide gives decision criteria to aid in selecting the best options. The following is guidance to be applied to technical manuals and other technical documents.

INTENDED DATA USE:

* select processable document architecture if documents

may require modifications or further processing in the future

* select processable document architecture if documents may be used in future document creation, e.g., for specialized documents

LIFE CYCLE PHASES:

* select document image files (e.g., raster scanned images) if large amounts of data already exist in hardcopy
* select processable document architecture if multiple authors (e.g., contractors) are participating in the development of the document

COST/BENEFIT:

* select magnetic tape for delivery of large volumes of digital data
* select integrated file formats for compound, multi-content documents

AVAILABLE TECHNOLOGY:

* select document image files if only minimal data processing capabilities are available internally

4. CONTRACT IMPLEMENTATION

There are six basic, yet non-exclusive, digital deliverable alternatives:

Deliverable and Form	Delivery Mode	Implement With
1. Document Image File	Magnetic Tape	MIL-STD-1840
2. Processable Text File	Magnetic Tape	DOD-M-28001 ref. by MIL-STD-1840
3. Raster Graphics File	Magnetic Tape	MIL-STD-1840
4. Processable Vector Graphics File - IGES	Magnetic Tape	DOD-D-28000 ref. by MIL-STD-1840
5. Processable Vector Graphics File - CGM	Magnetic Tape	CGM ref. by MIL-STD-1840
6. Integrated Text and Graphics File	Magnetic Tape or Telecommunications	ODA ref. by MIL-STD-1840

The existing functional standards are insufficient to invoke these alternatives contractually. Therefore, tailoring is

required when MIL-M-38784 is cited by the contract. The following are guidelines for tailoring MIL-M-38784 to obtain digital delivery of technical manuals:

* delete sections 3.2.2.4.1.3; 3.2.2.4.1.4; 3.6.1.2.1; 3.6.2.2; 5.1; 5.1.1; 5.1.4; and 5.2;

* substitute "digital data" for "camera ready copy" throughout the standard; and

* reference the applicable standard(s) shown in the table above for the appropriate alternative(s) chosen.

In addition, the tailored MIL-M-38784 should be referenced in Block 16 of Form 1423 to specify digital delivery in accordance with MIL-STD-1840. The physical media standards for magnetic tape delivery mode (shown in Appendix III - Contract Requirements for Delivery Modes) should also be specified.

TEXT

Federal Information Processing Standards Publication (Draft) on Document Application Profile for the Office Document Architecture (ODA) and Interchange Format Standard

CALS SOW TASK 2.2.2

Federal Information
Processing Standards Publication _____

(date)

Announcing the Standard for

DOCUMENT APPLICATION PROFILE (DAP) FOR THE OFFICE DOCUMENT ARCHITECTURE (ODA) AND INTERCHANGE FORMAT STANDARD

Federal Information Processing Standards Publications are issued by the National Institute of Standards and Technology pursuant to the Federal Property and Administrative Services Act of 1949, as amended, Public Law 89-306 (79 Stat. 1127), and as implemented by Executive Order 11717 (38 FR 12315, dated May 11, 1973), and Part 6 of Title 15 Code of Federal Regulations (CFR).

Name of Standard. Document Application Profile (DAP) for the Office Document Architecture (ODA) and Interchange Format Standard.

Category of Standard. Software Standard, Document Description, Electronic Document Interchange.

Explanation. This Federal Information Processing Standard adopts the NIST Implementation Agreement for a Level 3 Document Application Profile (DAP) for the Office Document Architecture (ODA) and Interchange Format Standard. The DAP facilitates the interchange of documents among different document systems by specifying the constraints on document structure and content according to the rules of the ODA Standard. The ODA Standard specifies rules for describing the logical and layout structures of documents as well as rules for specifying character, raster, and geometric content of documents, thus providing for the interchange of complex documents. The forms of the interchanged documents may be formatted form (i.e., for presentation such as

printing, displaying), processable form (i.e., for further processing such as editing) and formatted processable (i.e., for both presentation and further processing). The ODA Standard was developed by international standards organizations, primarily the International Organization for Standardization (ISO) and the Consultative Committee on International Telephone and Telegraph (CCITT). The Implementation Agreement for this DAP was reached by vendors and users of computer networks participating in the National Institute of Standards and Technology (NIST) Workshop for Implementors of Open Systems Interconnection.

Approving Authority. Secretary of Commerce.

Maintenance Agency. U. S. Department of Commerce, National Institute of Standards and Technology (National Computer and Telecommunications Laboratory.)

Cross Index.

a. International Organization for Standardization (ISO) 8613-1988, Information Processing - Text and Office Systems - Office Document Architecture (ODA) and Interchange Format Standard.

b. Stable On-going Implementation Agreements for Open Systems Interconnection Protocols, NIST Workshop for Implementors of Open Systems Interconnection, to be published.

Related Documents. Related documents are listed in the Reference

Section of the Document Application Profile.

Objectives. The primary objectives of this standard are:

- to promote interchange of documents between systems of different manufacturers,

- to facilitate the use of advanced technology by the Federal Government,

- to stimulate the development of commercial products compatible with the ODA Standard and with the Open Systems Interconnection (OSI) Standards,

- to contribute to the economic and efficient use of document processing system resources, and

- to avoid the proliferation of vendor-unique solutions.

Specification. Document Application Profile (affixed).

Applicability. The ODA Document Application Profile (DAP) is intended to be used by Federal Government agencies when acquiring document/text processing systems. This FIPS applies to systems ranging from the relatively simple wordprocessor (e.g., "What You See Is What You Get" (WYSIWYG) device) to more complex document processors (e.g., "desktop publishing" systems). Each system acquired by Federal agencies shall include appropriate system-to-DAP and DAP-to-system translators, such that incoming datastreams are interpreted correctly and that outgoing datastreams are generated correctly. Use of the DAP is independent of the communications used to transfer documents

produced by these systems; that is, the DAP may be used within the existing framework of communication protocols.

Implementation. This standard is effective (six months after date of publication of final document in the Federal Register). For a period of twelve (12) months after the effective date, agencies are permitted to acquire alternative software which provides equivalent functionality to the Document Application Profile. Agencies are encouraged to use this standard for solicitation proposals for new document processing systems to be acquired after the effective date. This standard is mandatory for use in all solicitation proposals for new document processing products acquired twelve (12) months after the effective date.

Waivers. Under certain exceptional circumstances the head of the agency is authorized to waive the application of the provisions of this FIPS PUB. Exceptional circumstances which would warrant a waiver are:

a. a justification for the waiver, including a description and discussion of the significant performance or cost disadvantages that would result through conformance to this standard as compared to the alternative for which the waiver is requested.

Agency heads may act only upon written waiver requests containing the information detailed above. Agency heads may approve requests for waivers only by a written decision which explains

the basis upon which the agency head made the required finding(s). A copy of each such decision, with procurement sensitive or classified portions clearly identified, shall be sent to the Director, National Computer and Telecommunications Laboratory, National Institute of Standards and Technology, Gaithersburg, Maryland 20899.

Where to Obtain Copies. Copies of this publication are for sale by the National Technical Information Service, U. S. Department of Commerce, Springfield, VA 22161. (Sale of the included references is by arrangement with the American National Standards Institute.) When ordering, refer to Federal Information Processing Standards Publication _____ (FIPSPUB_____), and title. Specify microfiche, if desired. Payment may be made by check, money order, or NTIS deposit account.

TEXT

ODA/ODIF Conformance Test Plan

2.2.3.1

ODA/ODIF Conformance Test Plan

This document discusses plans for testing conformance to the NIST Document Application Profile, a functional subset of the Office Document Architecture (ODA) and Interchange Format Standard. After a brief review of the ODA standard, the problems unique to testing document interchange formats are discussed, followed by a proposed test plan for ODA.

1. Review of the ODA Standard

1.1 Background

The recent growth in the use of personal computers and decentralized computing in the office allows users to create a wide range of documents containing, for example, text, images, computer graphics and data. This has emphasized the need to be able to transfer information electronically both within and between office systems.

There are two main aspects concerning the interchange of information:

- the communication protocols to be used;
- the format of the information to be transferred.

The first of these aspects is being tackled by the development of the OSI (Open System Interconnection) communication protocol standards. The second aspect can now be satisfied by the use of the ODA standard, to be published (in 1988) by the International Standards Organization (ISO) as ISO 8613 - "Office Document Architecture (ODA) and Interchange Format". The CCITT is also to publish an identical set of standards in the form of the T.410 series of Recommendations.

ISO 8613 and the equivalent T.410 series contain seven parts:

ISO 8613-1 (T.411):	Introduction and General Principles;
ISO 8613-2 (T.412):	Document Structures;
ISO 8613-4 (T.414):	Document Profile;
ISO 8613-5 (T.415):	Office Document Interchange Format (ODIF);
ISO 8613-6 (T.416):	Character Content Architectures;
ISO 8613-7 (T.417):	Raster Graphics Content Architectures;
ISO 8613-8 (T.418):	Geometric Graphics Content Architectures.

Part 3 was merged into part 2 during the development stage and is

reserved for future use.

1.2 Summary of ODA Functionality

The prime objective of ODA is to provide for the representation and encoding of documents so that they can be transferred between different systems regardless of their manufacture and location and of the operating system pertaining to those systems. Thus, ODA provides a means by which an originator and a recipient can have a common understanding of the data that makes up a document.

1.2.1 Forms of Transferred Documents

One of ODA's most important features is that it provides for the transfer of documents in two principal forms, namely "processable" form, which allows a document to be revised by a recipient, and "formatted" form, which is a form that allows the precise layout of the document to be specified. ODA also provides for the transfer of documents in "formatted processable" form; in this form the content of the document is represented in both formatted and processable forms at the same time. These forms are briefly described below.

a) Processable form documents

When a user creates and edits a document in a typical local text processing system, the content of a document is usually stored in what is referred to as processable form. In this form, the document has not yet been laid out in a form suitable for reproduction by an output device. A processable form document is one which is described in terms of its logical components.

The document may or may not contain information concerning how it is to be laid out and presented by the layout process. It may also contain rules and other information on how to edit the document. Interchanging documents in this form is thus very useful since the recipient can easily modify both its content and structure and can also modify the intended layout and presentation of the document.

b) Formatted form documents

A formatted form document is one in which the layout and presentation of the document are completely specified. Thus, a formatted document is one which is described in terms of its layout features and contains all the information required for an output device to print or display the document as intended by the originator. Documents in this form are not intended to be revised by the recipient.

This form is very useful when interchanging finalized documents

or other documents that are not intended to be modified.

c) Formatted processable form

This is the most powerful and versatile form provided by ODA since it enables a document to be represented and encoded in both processable and formatted form at the same time. That is, the document is described both in terms of its logical and layout features. In this form, a document can be edited and reformatted according to information specified by the originator or it can be displayed by the recipient as it was laid out by the originator.

The important feature of this form is that although both the processable and formatted forms of the document are interchanged, the content relating to both forms is the same and is only interchanged once.

1.2.2 Other ODA Features

Also, ODA provides for the representation of multi-media documents. At present ODA standardizes three content types: character text, raster scanned images and computer graphics. These content types conform to other existing standards.

In general, ODA provides features to support a wide range of different language and cultural requirements and thus the standard can be used for the world-wide interchange of electronic documents.

ODA encoded documents can be transferred using any form of communications, including storage media and OSI communication systems such as the Message Handling Service (MHS) and the File Transfer, Access and Management (FTAM) protocols.

2. Conformance Testing of Document Interchange Format Standards

The difficulty in testing conformance of standard document interchange formats lies both in the general nature of standards as well as in the scope of the specification of the standard. ODA specifies a generic data stream architecture for the interchange of a representation of objects, such as character text, graphics, and image objects. The standard, in general, does not focus on the method for generating or interpreting the datastreams. Instead, the scope of these standards addresses the semantics of a structure representing the interchanged objects and the syntax for a transfer format for the structured representation of objects.

2.1 What is Conformance?

Standards conformance generally means that the technical specifications defined are being met. In the case of ODA, conformance implies that the datastream adhering to the standard conforms to the prescribed semantics and syntax of ODA. This is often difficult to quantify and even more difficult to verify. To quantify conformance, what is needed is a clear measure of the parameters underlying the conformance statement; to verify conformance, what is needed is a practical means of confirming that the implementation produces results within the prescribed limits of the standard.

Like most standards, ODA is specified in descriptive prose, although a formal description is being defined. The problem with prose is its inherent weakness of interpretation. The value of conformance is depreciated if different, conforming implementations are able to be incompatible. Another characteristic making conformance testing difficult is that not all of the functionality is mandatory. Standards such as ODA provide optional features to increase the application of the standard to different uses. It is unlikely, however, that implementers will support all features. This raises the issue of which features of ODA must be supported in order to conform.

In addition, document interchange format standards -- like ODA/ODIF -- have a unique quality that makes verification difficult. Unlike protocol standards, such as those defined for Open Systems Interconnection (OSI), interchange format standards are "blind" interchange formats. No provision is made for specifying the process to be used for initiation or termination of an "interchange" session between an "originator" and a "recipient" of the datastream. Also, no provision is made for negotiating the set of semantic features to be used in describing the document. Lastly, no provision is made for exception condition reporting, handling, or recovery. Document interchange format standards merely specify the datastream to be exchanged between an undefined originator and an undefined recipient.

Under these circumstances, conformance testing of ODA/ODIF would seem to do little to assure interworking; however, experts working within the ODA community have provided a framework to complement the limited conformance specification of the standard. This has permitted the development of at least one practical approach to testing ODA conformance.

4. ODA Conformance

The ODA standard specifies conformance in terms of a conforming datastream. The datastream must either conform to the semantics and syntax of the standard as a whole, or the datastream must conform to a subset of ODA as specified in a Document Application Profile (DAP).

4.1 DAPs

ODA is a 'base' ISO standard which offers a wide range of choices of different sets of features. As a result, there has recently been much activity in the development of functional profiles that will specify subsets that are appropriate for particular applications. Subsets of the ODA standards are referred to as document application profiles (DAPs).

DAPs are expected to be published by various standards making organizations. For example, by CCITT in the content of telematic service Recommendations, by ISO in the form of ISPs (International Standardized Profiles) and by CEN\CENELEC in Europe as ENs (European Norms). Also, a number of user/manufacturer groups are now engaged in the development of a hierarchically related set of DAPs that will provide for the interchange of documents ranging from simple text documents to highly structured multi-media documents containing text and graphics. Examples of the latter are documents that can be produced using desk-top publishing systems.

The groups involved in this include the NIST (National Institute of Standards and Technology, Washington), EWOS (European Workshop for Open Systems) and INTAP (Interoperability Technology Association for Information Processing - Japan). Joint meetings of these groups are being held to produce internationally harmonized profiles for publication as ISPs. Also, it is expected that there will be close liaison with CCITT in this work.

4.2 FODA

The weakness of the descriptive prose specification of ODA has been addressed by the development of a formal specification for ODA; this project is called FODA - "Formal Description of ODA." The aim of FODA is to provide an unambiguous interpretation of ODA. FODA is intended to be used as a basis for implementing ODA, as a validation tool for verifying conformance of systems, and as a reference point for examining future extensions and revisions to ODA. FODA is a predicate calculus which defines ODA feature-by-feature and which can be processed in a straightforward manner by rules based on programming languages. This eliminates most of the interpretation weaknesses of the descriptive prose of the standard.

5.0 Test Plan

This section briefly describes the status of ODA testing and gives a proposed schedule for continuing the effort.

5.1 ISO Activities

In addition to FODA, ISO is currently studying ODA conformance testing methodologies and is developing software tools which will facilitate conformance testing.

5.2 TODAC Project

Since the process of generating and interpreting the ODA datastream is outside the scope of the ODA standard, ODA conformance testing is limited to an analysis of ODA datastreams. This makes the job of conformance testing easier for implementers; however, it does little to assure that implementations will be able to interwork with each other. To solve this, most ODA test architectures go beyond strict ODA conformance testing to provide additional tests that may aid in determining the likelihood of an implementation interworking with other, dissimilar ODA implementations. Such a verification method is being developed by a joint British/Canadian project. Called TODAC - "Testing ODA Conformance," the project is staffed by the National Computing Centre in the United Kingdom and the Department of Communications in Canada. NIST is a collaborator in this project; as such this project forms the basis of the ODA Test Plan.

5.2.1 IUT

Within the test architecture, an implementation is referred to as the Implementation Under Test (IUT). An IUT is categorized as either an originator, a recipient, or an originator/recipient class of implementation. The IUT is specified through the Document Application Profile along with an Implementation Conformance Statement (ICS). The ICS specifies the minimum requirements for the generation and interpretation of ODA datastreams.

5.2.2 Components of the Test System

The major components of the Test System are:

- a test document specification system - this system will create documents to test particular DAPs. Specific test cases, in the form of test document specifications, will be generated for an IUT by processing the requirements specified in the ICS and the DAP against generic test cases.

- an analysis system that checks that the structure and contents are valid for the ODA standard as well as the DAP. The Generation Test component will create verification test reports for originator class implementations. The test document specifications will be used as activity scripts for generating IUT results in the form of ODA datastreams. The Reception Test component will create verification test reports for recipient class implementations.

- a validated imaging system that produces reference images for comparison with the system under test. The reference document analyzer will process the output datastreams from an IUT and generate test reports.

5.3 Development Tasks and Schedule

1Q89 participate in preparing draft conformance methodology and test architecture, submit for draft proposed standard

first version of TODAC test tools ready

begin work on reference imaging system

participate in generation of abstract/generic test document specification

2/3Q89 ODA implementation(s) available for test, i.e., implementations to the NIST DAP; continue working with the NIST Implementors Workshop ODA SIG

complete TODAC tester available

participate in testing ODA implementations; begin with originator (generator) systems, then test recipient (interpreter) systems and originator/recipient systems

TEXT

PDLs: A Technology Assessment

CALS SOW TASK 2.4.1

PDLs: A Technology Assessment

The state of the Art
The state of ISO's SPDL

William T. Polk
National Bureau of Standards

ABSTRACT

Page Description Languages comprise a mature, well defined technology. Yet, as a group they are varied in both approach and functionality. A set of criteria are defined as a means to compare different PDLs. A brief survey of major PDLs is presented using these criteria. This paper attempts to define the present state of the art, and relate it to the ongoing International Standards Organization (ISO) project to develop the Standard Page Description Language.

1. Introduction

1.1 Purpose and Scope

This paper is intended to provide insight into the design of page description languages (PDLs). The paper primarily addresses the set of PDLs that are appropriate for device-independent description of compound documents. From that set of PDLs, the design choices made are identified and the ramifications explained. Some PDLs are less appropriate for the representation of compound documents, or contain device-dependent features. These PDLs are addressed to identify the design choices that reduce the functionality.

1.2 Overview

An introduction to PDLs and the basic definitions is provided. A set of criteria are defined as a means to compare different PDLs. A brief survey of major PDLs is presented using these criteria. This paper attempts to define the present state of the art, and relate it to the ongoing International Standards Organization (ISO) project to develop the Standard Page Description Language.

1.3 What PDLs are - and are not.

A Page Description Language, or PDL, is a language for unambiguous description of two dimensional images. The most flexible PDLs are device independent languages and allow for the inclusion of both text and graphics in the described image. These PDLs may be used to drive any type of presentation device: laser printers; graphic displays; or plotters. There are several types of PDLs, of varying sophistication. The most sophisticated PDLs are programming languages; the least sophisticated are static representations.

An *instance* of a PDL document, or *PDL instance*, is a non-revisable final form document. A PDL instance is the output of the Composition phase of the Document Production Process. A simple model for document processing is presented here as Figure 1. The composition system may involve formatting, translation and/or imposition. A PDL instance is created by the composition process by translating a formatted document (such as ODA final form), formatting an unformatted source document (such as an SGML document instance), or performing imposition tasks (e.g, n-up printing) on a formatted non-revisable document (such as a PDL instance). An instance will describe the one or more complete images, or pages, that make up the document. The pages may be rendered as sheets of paper, display screens or windows in a display. For a more thorough treatment of that process, see [ROSE].

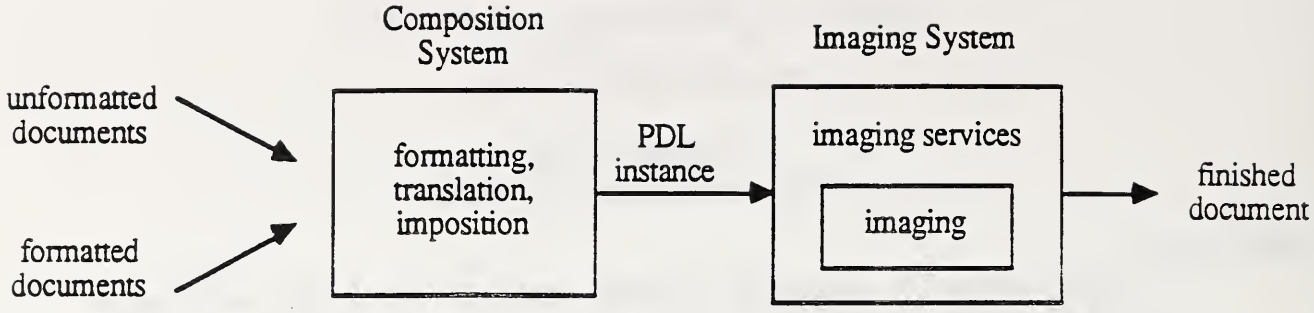


Figure 1. A simplified Model for Document Processing

An instance is submitted as input to an *imaging system.* The imaging system presents the document described by the PDL instance. There are two major categories of imaging system functionality - *rendering* and *imaging services.* Rendering is the process of creating the image on the display device. Presentation of the finished document may involve many operations that do not change the image rendered, such as binding, stapling or three hole drilling. The operations that change the presentation of the images, rather than the images themselves, are considered to be imaging services. (Imaging services are often known as *print services*, since most are specific to hard copy presentation.)

A PDL *picture* will describe a portion of an image, but is not by itself a legal PDL instance. A picture is used to facilitate "cutting and pasting" images in a document by applications. It is self contained and calls only the basic operators of the PDL and subroutines that are defined within the picture. A picture may be used to facilitate "cut and paste" operations; that is, to include images created in other applications at an arbitrary position in a page image. This allows use of a drawing package to create a figure, and inclusion of the figure in the text of a document. A picture may be defined explicitly in the specification for a particular PDL, but this is not always the case.

A *complete* PDL must be device independent, and be able to describe any image. To describe any image, the PDL must support both straight lines and curves of arbitrary widths, as well as colour. [Device independence is accomplished if the PDL and device have independent coordinate systems.]

[NOTE - PDLs are not completely non-revisable, PostScript programming and revision of PostScript documents are fairly common.]

1.4 Keywords

complete PDL - a complete PDL is device independent, and capable of describing any conceivable image.

device independence - a PDL is device independent if the page image is described without reference to any specific imaging engine

digital glyph - a bitmap or geometric graphics representation of a glyph

document - one or more page images intended to be presented together as a whole

document description - information that is not required for imaging, but describe the presentation of the document as a whole

font - a collection of glyphs having a characteristic design

font object - a font object is the imaging device's internal representation of a font resource

font resource - A font, together with attributes describing indivual glyphs (such as glyph name and glyph metrics), and a set of attributes associated with the font as a whole

glyph - A recognizable shape that conveys meaning to the human brain

glyph name - a name associated with the glyph as an identification mechanism

glyph metrics - the set of measurements associated with the glyph

imaging device - printer, plotter, terminal or workstation display

instance - a PDL instance is a complete description of a document as a series of one or more page images

page description language (PDL) - a special purpose language intended for the description of two dimensional images

page image - a page image describes a single complete image, intended to be viewed as a unit

page independence - a PDL is page independent if a page image can not be affected by the previous page image in the instance

picture - a PDL picture is a procedure, or function, that describes a portion of a page image.

resolution - the precision of the device; for example, dots per inch for displays and laser printers

These definitions correspond where possible to the definitions used in ISO/IEC JTC1/SC18 N1402 (SPDL, 3rd Working draft.), the definitions used in the current draft of DIS 9541 (Font Standard), and ISO/IEC JTC1/SC 18 N 1370 (Computer-Assisted Publishing - Vocabulary.) Definitions have been modified where such modification aids the understanding of the reader. The terms *PDL instance* and *complete PDL* are terms invented for this document.

2.0 Comparison Criteria

The three major areas of comparison for PDLs are the operational model, functionality, and efficiency. These areas are interdependent. Design choices in any one of these areas will be reflected in the other two.

The operational model chosen for a PDL will affect the functionality and efficiency of the resulting product. Note that the operational model is not necessarily utilized in any implementation.

The functionality of a PDL is its list of capabilities, i.e, what it can and cannot do. Functionality in terms of text support, types of graphics (if any), extendability, and document description are of particular interest.

The efficiency issue is a particularly difficult matter. Efficiency is closely linked to the operational model and functionality of the PDL; certain design choices in the model and functionality will always have a negative effect on the efficiency. On the other hand, efficient language design does not guarantee an efficient implementation. This paper will address inefficiencies in design, but it will make no attempt to address inefficiencies in implementation.

2.1 The Operational Models

There are two major types of processing models for PDLs: the static representation; and a programmable model. The static model contains a fixed set of commands, which may not be extended by the end-user. The static model is basically analagous to programming in an assembly language without branches or jumps. A programmable model will typically contain branches, loops and jumps and may allow the set of commands to be extended by creation of functions or procedures.

In general, programmable PDLs have advantages of additional flexibility, extensibility, and a more compact and efficient document instance than static PDLs. It is generally easier to "cut and paste" fragments in a programmable PDL than in a static PDL.

2.1.1 Static

A static PDL has no procedures, loops, jumps, or conditionals. The interpreter for a static PDL consists of only two parts: the current state; and the unread input string. The consumed input string is not of interest. The advantages of this design are efficient execution and parsing, and assurance of terminating code. The disadvantages are large document instances, limited flexibility, and lack of extensibilty.

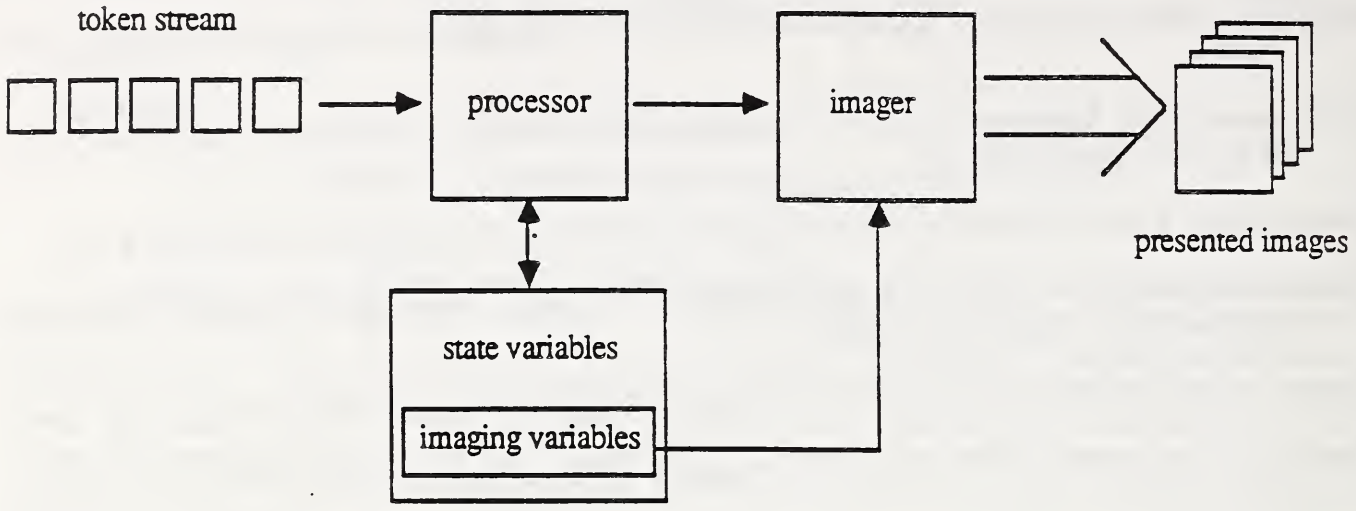


Figure 2. Basic Operational Model for Static PDLs

The basic operational model of a static PDL is shown as Figure 2. The model consists of an input, an output, a set of state variables, a processor and an imager. The state variables are a finite set of variables defined by the PDL. The set of values usually includes such items as "current font" or "current position". The processor consumes tokens from the input and executes the operators. Processor execution will modify the values of the state variables. The imager renders the finished page images by directions received from the processor, utilizing values from the state variables. (For a device dependent, static PDL, there may be a single unit performing both the processor and imager tasks. This is due to the simplistic imaging model (Section 2.2.6) of device dependent PDLs.)

An instance of a static PDL will consist of a series of operators and parameters. Each operator is executed in turn. Neither the previously consumed input string or unread string is of any interest in the execution of that operator. The execution of the operator will depend on its parameters, and might depend on a set of state variables maintained by the imaging system. While the values of the set of state variables is a function of the consumed input string, the function is many-to-one. That is, many input strings can create the same set of state variable values, and it is unnecessary for the processor to know how that state was reached.

2.1.1.1 Object/Attribute Lists

State variables are not strictly necessary for static representation for fully formatted documents. The special class of static representations without any state variables is the object/attribute list. In this class of document representations, all attributes are listed with each object. A document instance of an object/attribute list is simply a list of all primitive objects in the image[s], along with their attributes. The object/attribute list representation is not thought of as a PDL, since it is really not a language. An object/attribute list representation is strictly a series of operators with all necessary attributes.

The state of the interpreter for an object/attribute list is completely defined by the unread input string. The operational model for static representations is modified by removing the state variables. Branches and jumps are not supported (hence, the word 'list') and access to a stack or memory is unnecessary since there are no variables.

Object/attribute lists are the simplest representation of fully formatted documents. They are somewhat less flexible than static PDLs, and are less efficient in certain ways. Availability of state variables can reduce the size of the document instance, since some information can be assumed. The reduction in tokens can lead to a substantial reduction in the overhead for parsing. The ability to save and restore the state of the system is lost in an object/attribute list. There is an elegant

simplicity to this class of document representations, however, and object/attribute list laser printers are among the least expensive on the market.

2.1.2 Programmable

Programmable PDLs resemble general purpose programming languages in many respects. An instance of a programmable PDL is actually a computer program written in that PDL. The instance may include the creation of procedures, have control constructs (conditionals and loops), computing constructs (arithmetic operations), stack manipulation and variables. Unlike a static PDL, a programmable PDL allows reference to objects defined in the previous input string. There are two main approaches to designing programmable PDLs.

The first approach is to provide the programmer enough tools to write general-purpose programs. The emphasis in the design is on flexibility and programming power. No attempt is made to ensure that inefficient or non-terminating code cannot be created. An example of a PDL with general purpose functionality is PostScript[2], which provides a control operator (loop) that may easily result in an infinite loop. Essentially, this approach is to augment the special purpose operators for image description with the functionality of a general purpose programming language.

The second approach is to provide only those tools required for the task of creating a PDL instance, and to avoid providing any tools that might be misused. Any feature that might result in a non-terminating instance would be removed from the specification. The emphasis in this design strategy is on efficiency, speed, and reliability. (This approach is favored by builders of high-volume, high-cost printing systems.) An example of this approach is Interpress[1], which provides no looping constructs at all.

The difference between the two approaches is not in what can be described, but rather how it may be described. For example, a loop can be simulated in Interpress by creating a procedure containing the loop's contents, and calling the procedure a series of times, or with recursion (this option is somewhat inefficient). Since it is non-trivial, a systems programmer would require a very good reason to create such a document instance in Interpress. A systems programmer might routinely use a PostScript loop to create images that the Interpress designers felt should be done otherwise. Both PDLs can conceptually describe any possible page. The ease with which it can be described will differ, however.

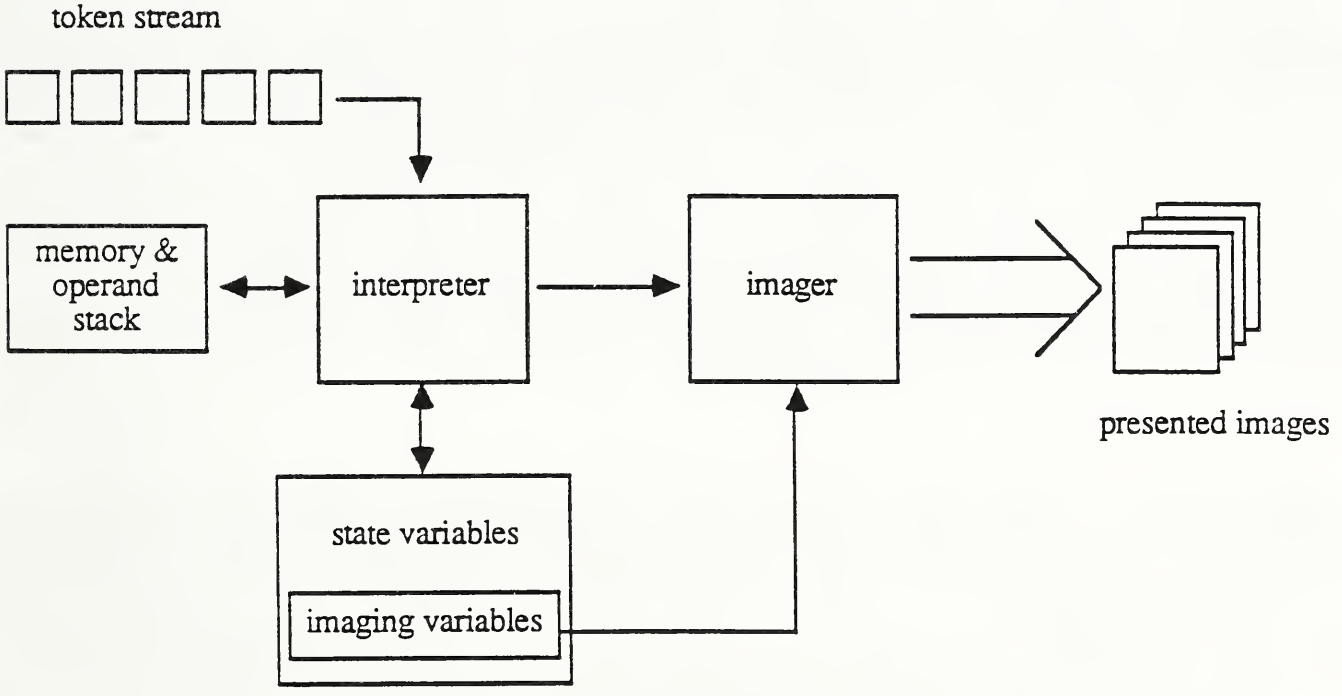


Figure 3. Basic Operational Model for Programmable PDLs

---

[1] Interpress is a trademark of XEROX Corporation.

[2] PostScript is a trademark of Adobe Systems Incorporated.

The basic operational model of a programmable PDL is similar to that of static PDLs. It does include an additional feature - a memory store. A fixed number of variables, if any, may be allowed by a static PDL. Since these are defined in the language specification, they may be considered state variables. So, no memory store is required for static PDLs. However, an instance of a programmable PDL may include declared procedures, structure definitions, or variables declarations. A memory store is required, since these instance-specific objects may be referred to later in the execution of the instance. Note that the "processor" block has been relabeled "interpreter" as well. Since there are no declarations in the static PDL instance, there is nothing to interpret - all operators may be directly executed.

[NOTE: The models given as figures 2 and 3 represent the processing models corresponding to the language designs, but are not necessarily similar to the actual implementations of all PDL processors. However, the semantics implied by the structure of the models must be implemented to realize the semantics of the PDL.]

An instance of a programmable PDL is actually a computer program written in that PDL. The instance may include procedure definitions, variable declarations, and references to system resources. The imaging system must maintain a working knowledge of previous stuff, since references will occur to previously defined objects (such as procedures) "later" in the execution of the instance.

2.1.2.1 Stack Oriented

Most of the major programmable PDLs (including Interpress, PostScript and DDL) are postfix notation, stack oriented processing languages. Stack oriented PDLs offer advantages in execution efficiency, since they may be parsed without any lookahead. The operational model that corresponds to this design is the same one shown in Figure 3. As a zero lookahead design, this model lends itself well to efficient implementation.

2.1.2.2 Structure/Page Independence

Like other programming languages, the question of structure is a key decision in the design of programmable PDLs. Unlike general purpose programming languages, the PDL concept of a structured language is closely related to the concept of a structured document. A structured PDL requires the program be divided into a document, page(s), and picture(s).

The most important concept of structured PDLs is that of *page independence*. A PDL is page independent if a page image can not be affected by a previous page image in the instance. This allows implementors to build systems which interpret multiple pages in parallel. This is an important feature if the PDL will be used for demand printing. (Note: Static PDLs may also exhibit page independence if they revert to a default state after each page is rendered.)

Structured PDLs have several additional advantages. It becomes much easier to support "cut and paste" operations, so that importation of images developed in other software systems is reliable and straightforward. Structure also allows the hierarchical inheritance of attributes. Finding and correcting errors is simpler for systems developers, just as it is easier to debug programs written in structured programming languages. The basic disadvantage would appear to be the increased complexity of the interpreter (2-stage rather than 1).

2.2. Functionality

Functionality and capability of a PDL are the set of design choices that affect what the PDL can describe and how difficult it is to do so. Key areas are graphics, text, fonts, extensibility, document description and imaging model. A complete PDL can describe any possible page in a device-independent manner.

2.2.1 Graphics

There are two approaches to graphics; 1) the lowest common denominator approach, where instructions describe objects all imaging systems can render exactly, and 2) where the PDL describes an ideal image, and all imaging systems render the image with the best approximation they can get. In the "lowest common denominator" approach, a PDL will handle only raster graphics. To be complete, an "ideal image" PDL must provide at the minimum the capability to

draw curves and straight lines of arbitrary width, and fill closed paths. This allows any arbitrary image to be described in a device independent fashion. That is not possible for a PDL with only raster graphics. If the resolution of the printer is greater than that of the raster image, this method will not produce the most accurate representation of the image possible. PDLs without ideal image support tend to be used with a single target device.

Note: It is insufficient for a PDL to represent curves as a series of straight lines in a PDL. This solution requires that a guess be made about the printer resolution when the instance is generated. When a printer attempts to render the image, it will be approximating straight lines rather than a curve. This can result in images that are not the best possible for that print engine.

2.2.1.1 Geometric Graphics

Geometric graphics provide the ability to define and draw bezier curves and fill closed paths. Geometric graphics are usually in the "ideal image" realm.

There are usually four groups of commands: one to draw curves (a straight line is a degenerate curve); a second to define a path; a third to sketch the outline of a path; and a fourth to fill areas inside a closed path.

Additional commands to produce lines and arcs may be available to increase ease of programming. These are of course just special cases of the Draw Curve command.

The image described by the path may be simple shapes, such as lines or curves, or a closed curve defining an object. In some PDLs, the object may be a disjoint set of curves, such as two concentric circles forming a donut. In the case of an object, the "inside" is defined by the rules of geometry (odd-even rule or non-zero winding rule).

2.2.1.2 Raster Graphics (Bitmap)

Raster, or bitmap, graphics are essentially the description of images by specifying the colour of each pixel. Raster graphics are essential for efficient support of scanner images.

Simple printers without geometric graphics may use bitmap graphics for all non-text information. These printers require that the bitmaps have a resolution equivalent to, or half of, that of the printer. This creates large instances, but requires little or no calculations by the printer. In this case, the PDL is device dependent.

Complex printers may allow bitmap graphics for all resolutions up to that of the printer. This is a more flexible and device independent solution, but it requires many more calculations by the printer. These printers usually have geometric graphics, and the bitmap graphic support is intended for use with scanner images only.

2.2.2 Text

All PDLs provide direct text support. That is, they supply data structures and operators for imaging text efficiently. Direct support for text is not technically required for a PDL to be complete. The character glyphs are, after all, simply graphics that the viewer associates with a distinct concept. Therefore, it is not necessary to provide separate support for text to describe any possible page. Such PDLs do not exist due to the performance liabilities of such an implementation.

The performance liabilities of a PDL without direct text support are a function of the size of the document instance. Textual representation of a character in the PDL instance typically requires only 8 bits for western languages (such as English), and 16 for the Eastern languages (such as Kanji.) Direct text support often includes operators handling strings of characters. Direct text support enables vendors to build printers with fonts in hardware, which is an opportunity for considerable performance enhancements in terms of both size and execution. Pictorial and geometric representations are several orders of magnitude less efficient than textual representation, since they may not handle more than one character per operator. The costs in storage and transmission, as well as the transmission time, are too large to justify the simplification.

Direct text support involves one data type and a set of instructions. The data type is the "font object". Fonts are covered in depth in the following section. The instructions are typically variations on "render character" and "render string". At one extreme, some PDLs offer only "render character." The other extreme is the set of PDLs which include a "render string, justified"

or allow rendering of justified text by altering state variables. String support trades some typographic quality for an increased efficiency. The appropriateness of such support is still an open question. Extremely high quality typographic output will typically require placement of each character individually; the majority of the world's documents can presently be supported by rendering text as strings. Whether such compromises will continue to be acceptable is an open question.

2.2.3 Fonts, Font Resources, and Their Parts

A *font* is a collection of shapes, known as *glyphs*, and information about the individual glyphs and collection as a whole. The information about the font might include such attributes as character collection (included glyphs), body size (e.g, 10 or 12 point) and font family (e.g, Helvetica or Times-Roman). The font may also be characterized by the type of glyph representation as a *raster font* or *outline font*.. This is called *shape technology*. Individual glyph information would usually include net escapement (the relative change of the current point after imaging a glyph), the weight (the space the glyph appears to fill) and the glyph name.

Information about fonts can be obtained from three external resources. The *font resource* contains raster or pictorial representations of the glyphs, or shapes, of the characters in the font. Font resources contain additional data items pertaining to character metrics, which are collectively known as font metrics, and glyph name to glyph mappings. The font metrics address spacing of characters by specifying a default origin modification. This information automates the placement of characters (vertically and/or horizontally for Asian languages, horizontally for Western: directional character spacing as required.) This information increases the efficiency of direct text support. The *code map* contains an identifier to glyph name mapping. The font metrics may also exist independent of a font resource.

When the PDL is interpreted, the textual representation will be resolved, and the appropriate image rendered using information in a *font object*. A font object is a black box maintained by the printer, and contains glyph information, character metrics, and an identifier to glyph mapping. Font objects may be created in several ways: they may be created from a font resource and a code map; a font object may be modified by a new code map; and a font object may be modified by a set of font metrics.

Code maps are a many-to-one mapping from an identifier(s) to a glyph name. Glyphs and Identifiers are unique, but several glyph names may correspond to a single glyph. This implies that several identifiers may correspond to the same glyph for a given font object. This is useful for glyph substitution, and Kanjii text. In glyph substitution, you may wish to use a hyphen if the font lacks a neutral dash, but still use a hyphen. In Kanjii text, the same character must appear with support for multiple writing directions. In either case, a mapping from several ids to a single glyph is quite useful.

In addition direct text support may be more efficient than geometric graphics, since the shapes may be stored as bitmaps. This is because the repetitive quality allows the software to save the bitmaps created from the geometric shape. This means the following application of the character will not require creation of a bitmap. This is commonly called *font caching*.

Font objects are created from font resources and code maps. Font resources contain glyph descriptions, glyph name-to-glyph maps, and font metrics.

2.2.3.1 Bitmap Fonts

Bitmap fonts are usually intended for use at a specific point size. This means the bitmap representations of the glyph shapes in the font can be easily tuned to obtain the most attractive shape possible at a particular resolution, or for a specific print engine. This is an important advantage, since font selection is basically a question of aesthetics. Ugly fonts are not tolerated by any but the most casual users.

There are several strong disadvantages to this approach. As bitmaps, they cannot be scaled or rotated easily, and the results may be very unattractive. The font may not be portable to other printers. If the font can be ported, differences in resolution of print engines may negate the aesthetic advantage of tuned bitmap fonts. Machine dependent fonts limit the number of suppliers in the market.

2.2.3.2 Geometric Fonts

The geometric fonts are a more flexible representation than bitmaps. This flexibility brings a number of advantages. It reduces the number of fonts required, since the point size can be adjusted by scaling. More general two dimensional transformation (scaling, rotation and/or translation) of geometric fonts is also possible, and provides predictable results. Geometric fonts are generally more portable than bitmap fonts, since they contain no information about specific print engine resolutions.

Geometric fonts have an ideal size, but are usually intended for use throughout a range of point sizes. This implies that compromises must be made so that the font will be reasonably attractive at all resolutions and sizes. Scaled geometric fonts will often will be less attractive than the hand-tuned fonts designed specifically for that point size.

In general, a 20 point font is not simply twice the size of the 10 point font from the same family. The basic shape of the glyph is the same, but minor adjustments are made. To overcome this problem, some PDL interpreter vendors encode hints for adjusting the shape after scaling to obtain the most attractive scaled fonts. This information is proprietary, and means that that portion of the font is non-portable. Scaled fonts on different printers may look different if one utilizes hints unavailable to the others. This also means that fonts must be bought from the PDL vendor if the user intends to scale them, and has a critical eye.

2.2.4 Flexibility/Extensibility

In general, programmable PDLs are user extendable. Static PDLs are not. Extensibility has several advantages. Extensibility allows the user to in some effect add basic operators to handle new content architectures and to adapt the system to handle their specific needs. When used properly, this feature can result in greater efficiency in terms of storage and programmer productivity (as discussed in sections 2.3.1 and 2.3.3).

2.2.5 Document Description

In some cases, page description language is a misnomer. Such PDLs as Interpress, SPDL and DDL can/will in many ways perform document description as well as simple image description. In Figure 1, the imaging system is shown as the combination of imaging services and rendering. The imaging services do not affect the images rendered, but do affect the presentation of that series of images. Imaging services might be 3 hole drilling, binding, or stapling.

Information imbedded in a PDL instance that does not affect the rendering of the document's page images, but require presentation services are considered to be document description. Existing proprietary PDLs have chosen widely divergent paths in this area. Some PDLs allow considerable document description information (examples include DDL, and to a lesser extent, Interpress); others include no document description at all (PostScript, DVI and PCL). Even now, there is no clear consensus about how much document description should be included in a PDL.

2.2.6 Imaging Model

The simplest possible imaging model is the model for a device dependent PDL describing only black and white images. This model consists of a single plane, with a device dependent coordinate system corresponding to the resolution of the device. Images are described in terms of that plane, and applied to the display device exactly. The device dependent plane is called the *image plane*.

The imaging model for a device independent, black and white PDL has at least two planes. The two planes have independent coordinate systems. The image is described in terms of one plane, called the *mask*. The second plane is the image plane. A coordinate translation and accomadations for the resolution of the device are made when applying the mask image to the image plane. This model allows a document instance to be rendered on devices with differing resolution.

The image described in the mask may contain simple shapes, such as lines or curves, or a closed curve defining an object (which may be filled with some pattern). In some PDLs, the object may be a disjoint set of curves, where the "inside" is defined by the rules of geometry (odd-even or right hand rule). This is a function of the graphics model, rather than the imaging model. The

image described by the mask in figures 4 and 5 is a disjoint curve purely for effect.

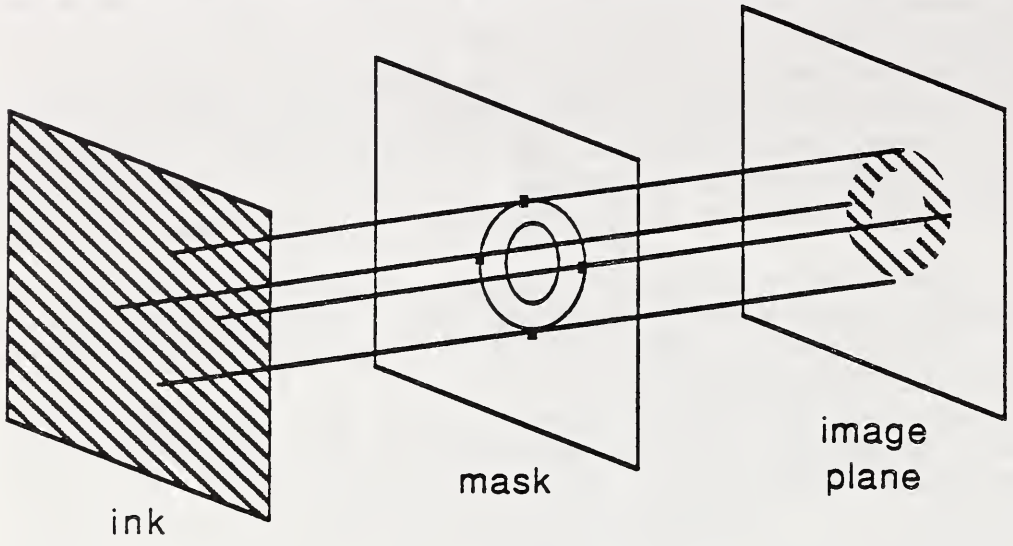


Figure 4. A minimal imaging model for a device independent colour PDL

The model for a device independent PDL supporting either colour or grayscales has at least three planes. The two-plane model is augmented by an *ink* plane. The ink plane describes the colour or texture that is to be applied to the image described by the mask. Texture may be any pattern; for example, the ink plane might be solid red, the "Mona Lisa", or a rainbow pattern. The Ink plane is normally described in terms of the coordinate system of the mask. (If the ink and image planes shared a coordinate system, the PDL would not be device independent.)

The pattern described may be opaque, translucent, or clear, depending upon the PDL. The modifications made to the image plane will be different in each of those cases. If the ink supports only opaque colours or patterns, the application of the mask and ink will cover that section of the image plane. If the ink plane supports translucent colours, the image will be additive, so that blue and red intersect as purple. If the pattern has a clear section, that portion of the image plane will remain unchanged.

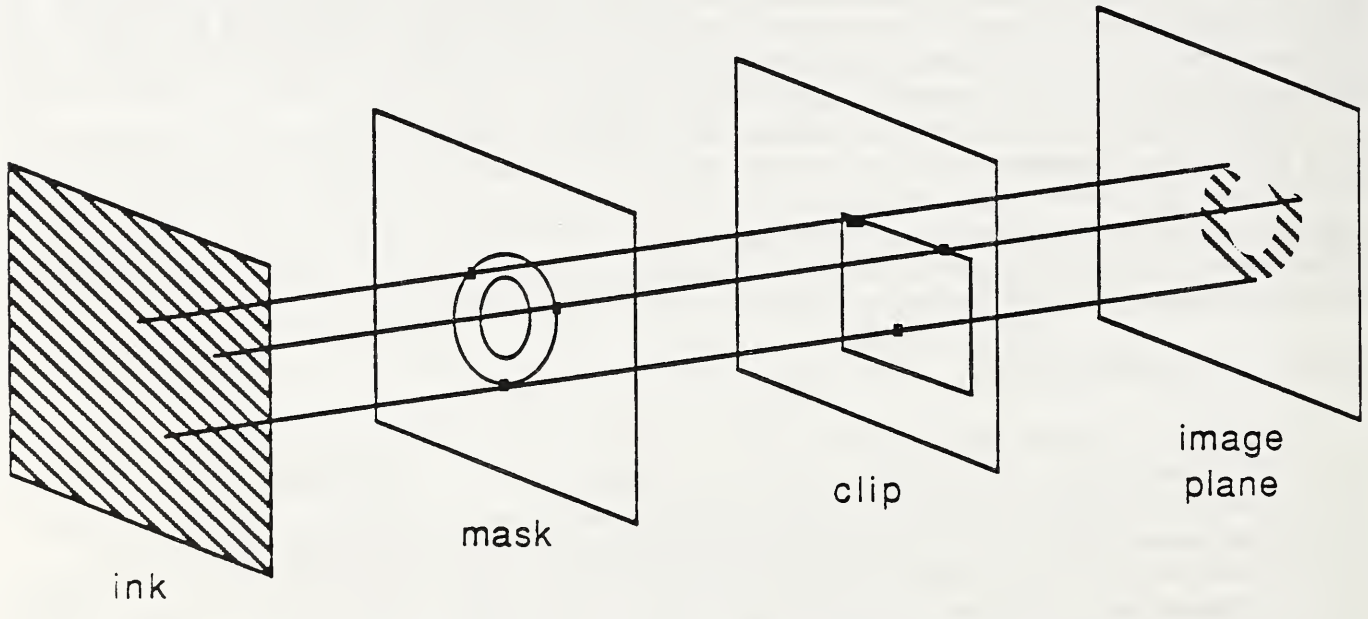


Figure 5. A richer imaging model for a device independent colour PDL

Device independent PDLs may augment the imaging model with a *clip* plane. Like the ink plane, the clip plane is described in the same coordinate system as the mask plane. The clipping region is a persistent description of the area of the page image which may be altered. The clipping plane is not necessary to describe any image, but is useful to limit the portion of the image plane that may be modified. This allows the insertion of PDL fragments into an instance without interpreting the token stream to verify the size of the image described. (The clipping region

typically is initially the page area.)

2.3 Efficiency

There are three different types of efficiency: storage and transmission efficiency, which is dependent upon the size of the PDL instance (which is dependent on the operational model, encoding and features); execution time efficiency, which depends on features and implementation; and programmer productivity efficiency, which is the ease with which the desired PDL instance can be created.

2.3.1 Storage/Transmission

In general, human-readable forms are less efficient than encoded forms. PDLs that have direct text support are literally thousands of times more efficient. Programmable PDLs are more efficient than static PDLs. By extending the basic language to meet the particular needs, redundant code may be replaced by procedure calls.

2.3.2 Execution Time

Encoded forms are more efficient than human-readable forms, since parsing is much simpler. Static forms are simpler and more efficient to execute, since there is less overhead - there are no scope rules to implement, no conditionals to perform, and no jumps. A static form implies that only the present state and the unread input string are of interest - any part of the document instance that has been executed may be forgotten. PDLs supporting raster shape fonts are more efficient than geometric shape fonts, although the difference is negligible if a cache of bitmaps is maintained.

Execution time can also be reduced by building multi-processor systems if the language is page independent.

2.3.3 Software Development/Programmer Productivity

PDLs are not intended for use as general purpose programming languages, but analogies to classical programming languages are helpful. High-level languages are more efficient for system developers than assembly language, and so it will be easier to develop code for languages with powerful control structures. In general, human-readable forms are more efficient for system developers than encoded forms, i.e, mnemonic assembly is far easier to program in than machine code. (Some of the difficulties can be somewhat offset by PDL disassemblers and macro substitution.) Creation of complex programs with programmable PDLs will be simpler and faster than with static PDLs.

3.0 The current state of the art

This section provides a brief overview of currently of popular page description languages. The systems are described in terms of the comparison criteria defined in section 2. A summary of the results are also given in table 1.

3.1 Interpress

Interpress was designed in 1976 by Xerox [INTE]. Interpress was designed for use on high-speed, high-volume printers. Consequently, a machine-encoded form was chosen to increase efficiency. Interpress is a programmable, stack-oriented language, but it is not a general purpose language. When a trade-off between efficiency and functionality was considered, efficiency was chosen. One example is that Interpress lacks looping constructs. The philosophy was, "if you can't write a loop, you can't write an endless loop."

Interpress is a complete PDL - it is device independent, describes any conceivable page, and supports both raster and geometric graphics, as well as outline fonts. Interpress is page independent, and includes document description information. The Interpress graphics model does not support disjoint paths.

Interpress uses a three plane imaging model. The three planes are the Color, Mask, and Page Image planes. The Color plane (the ink in the model presented in section 2.2.6) supports any opaque colour and "transparent" but does not support patterns.

PDL (company)	Operational Model	Graphics		font shape technology		Imaging Model		encoding	
		raster	geometric	raster	geometric	device independece	supports clipping	machine readable	human readable
InterPress (Xerox)	Programmable Stack Oriented	✓	✓	✓	✓	✓	✓	✓	
PostScript (Adobe)	Programmable Stack Oriented	✓	✓	✓	✓	✓	✓		✓
DDL (Imagen)	Programmable Stack Oriented	✓	✓	✓	✓	✓	✓	✓	✓
DVI (Donald Knuth)	Static Representation	✓		✓		✓	✓	✓	
PCL (Hewlett Packard)	Object/Attribute List	✓		✓			✓	✓	

Table 1. PDLs and the Comparison Criteria

3.2 PostScript

PostScript was designed in 1982 by Adobe Systems [POST]. PostScript was designed with the over-riding concept that a PDL should provide all the functionality of a general purpose language. The human-readable encoding was chosen to make system development easier. PostScript is a complete PDL, supporting both raster and geometric graphics, as well as outline fonts. Postscript is available on a wide range of devices, ranging from color 300 dpi laser printers to 2500 dpi typesetters to workstation display devices, although selection is heavily weighted towards 300 dpi, low-volume, low-speed laser printers.

PostScript uses a four plane imaging model. The four planes are the ink, mask, clip, and image planes. The Ink plane supports any solid, opaque colour but does not support patterns. The PostScript graphics model supports disjoint paths, and includes support for both the even-odd rule and non-zero winding number rule to determine the "inside" of an object.

Pictures are not explicitly defined in the PostScript specification. There is an accepted specification for PostScript pictures, called *Encapsulated PostScript*, but the definition is advisory and not enforced by the language itself.

PostScript is not structured, and is not page independent.

3.3 PCL

PCL[3] was developed by Hewlett-Packard. PCL was designed to drive low cost, low speed printers to present documents made up largely of text. With these goals, an object/attribute list

[3] PCL is a trademark of Hewlett-Packard.

representation was chosen, rather than that of a page description language. While PCL is the least ambitious design examined here, it should be noted that there are more PCL printers in use than the other PDLs combined. PCL clearly dominates the low end of the laser printer market (The list prices of PCL printers range from approximately $2,000 to $3,000.)

PCL supports only non-scalable bitmap fonts. PCL supports raster graphics, but has no facilities for geometric graphics. The coordinate system is fixed. As such, PCL is an incomplete and device-dependent representation.

PCL uses a two plane imaging model. The two planes are the mask, and image planes. There is an implied Ink plane which supports any solid colour as long as its black.

3.4 DVI

DVI was designed in 1979 by David R. Fuchs to support high-quality electronic typesetting for text documents [KNUT]. As such, DVI includes only the functionality required to produce very high quality text output in any language. In fact, 208 of DVI's 250 commands are for text support. 136 of its commands are for character placement. Of the remainder, 68 are for setting the current font, and 4 are for font definition.

DVI includes the concept of state variables, and has 28 commands for manipulating them. DVI also includes push and pop commands to allow the state variables to be saved and restored. DVI may be classified as a page description language based on this support of state variables. DVI is not a programmable PDL. There are no features that allow the systems developer to define new commands.

DVI does not support string text operations. Since high quality typesetting requires positioning each character precisely, this is not a problem for the intended audience. Graphics were not considered a priority, and in fact DVI supports only imaging of black rectangles. As such, DVI is incomplete, despite utilizing a device independent imaging model.

A static representation, machine-encoded form was chosen. This architecture maximizes the processing-time performance gains available in comparison to a programmable form. It also means that DVI document instances may be quite compact.

3.5 DDL

DDL[4] was developed in 1986 by Imagen. DDL (Document Description Language) was intended to cover the entire spectrum of printing systems by providing two parallel encodings. One encoding was human readable, the other was machine-encoded. DDL is a stack oriented programmable language, and is complete. DDL supports both outline and bitmap fonts, and allows scaling of both. As the name implies, DDL includes a lot of document description information. DDL is a highly structured PDL, with an outer level syntax separating the preamble and various sections. The inner level syntax is then interpreted separately. DDL implementations have only recently come onto the market. It is unclear if DDL will make inroads, or in what sections of the PDL market.

DDL includes two languages, the Document Layout Language (DLL) and the Document Control Language (DCL) which are expressly for the purpose of declaring a document's printer requirements (duplex, colour, etc.) and embedding information about the processing involved (who spooled the job, and when they did so, etc.), respectively. This is a large departure from the previous PDLs.

DDL has many tools for the system developer. DDL includes loops, branches and case statements for execution control and seven data types. DDL uses an imaging model unlike that of other PDLs. Most PDLs allow creation of a path, and then it is applied to the page image. DDL allows the creation of composite objects, which are basically multiple paths, their associated transformations, and ink definitions. This allows very complicated objects to be treated as primitives.

DDL does not seem to provide an overwhelming reason for vendors to migrate from the PDLs they currently support. It would seem that the key players will wait for SPDL, and simply continue to protect their current market.

---

[4] DDL is a trademark of IMAGEN Corporation.

4.0 The SPDL project

The SPDL project is an ongoing work item of ISO/IEC JTC1/SC 18, Working Group 8 [SPDL]. The corresponding ANSI committee is ANSC X3.V1 Task Group 8. American participants include Adobe Systems, DEC, Hewlett-Packard, IBM, Lawrence Livermore, NIST and Xerox. International participants include England, ECMA, Germany and the United States.

The objectives of the SPDL project were to specify the syntax(es) and semantics of a PDL that would be appropriate to cover the entire realm of the electronic printing industry. The SPDL project was designed to standardize a mature industry, and allow greater interoperability of products (composition systems and imaging systems). These goals require a complete, device independent page description language. If the standardization process works well, the prices should drop and the market should expand.

SPDL's current schedule is distribution for voting as a draft proposal in January of 1989, followed by a vote for Draft International Standard in January of 1990.

4.1 SPDL and the Comparison Criteria

SPDL will be a programmable, stack-oriented PDL. SPDL will be a highly structured language, with constructs for document, pages and hierarchically nested pictures. SPDL will be page independent. SPDL will be an effective compromise between the opposing camps on general-purpose functionality. For example, it will probably contain constructs such as loops, but the loops will have a fixed number of iterations. These types of compromises will allow SPDL to provide most of the functionality found in general-purpose programming languages but make it difficult to write non-terminating code. It will support both raster and geometric graphics. There will be two encodings, a human-readable form, and a machine encoded form. Such compromises may not satisfy everyone, but prevent anyone from being particularly unhappy.

SPDL uses a four plane imaging model. The four planes are the ink, mask, clip, and image planes. The Ink plane supports any colour or pattern. It is still unclear if the Ink plane will only support opaque colours, or if translucent colours and "transparent" or clear will be supported as well.

SPDL presently provides direct text support in terms of three imaging operators, fonts and code maps. The three imaging operators are *showcharacter*, *showstring*, and *showescapedstring*. Showstring adjusts positions using the default values embedded in the font object. This is very efficient, and the quality is sufficient for most documents. Showescapedstring explicitly adjusts the position of each character, allowing high-quality typesetting to take advantage of the efficiency of string operations. Operators are included to allow the creation, modification and transformation of fonts. SPDL's font support will certainly include both bitmap and outline fonts.

SPDL straddles the fence on the efficiency issues. The efficiency issues are determined by a few important points - the encoding, the operational model, and the overlap with general purpose programming languages. Having two encodings allows the user to choose the SPDL form that is most efficient for his application. The functionality overlap with general purpose programming languages falls between that of PostScript and Interpress. The postfix notation execution model is a widely used and well understood model. While that is not as as efficient as static PDL execution, the PDL instances will be more efficient (i.e, smaller) than the static PDL instances.

4.2 How SPDL relates to the major proprietary PDLs

SPDL follows the conventional wisdom in most ways. It is a stack oriented, programmable PDL. SPDL's ink plane presently supports any opaque textures. Support for screening colors is also under consideration. SPDL will support disjoint paths with at least one method of specification of "inside", and may support both.

The execution time efficiency of machine encoded SPDL should rival that of Interpress. SPDL does include more general programming features than Interpress, but the preliminary indications are that the cost will be minimal. The execution time efficiency of human-readable SPDL should at minimum rival that of PostScript. PostScript does include more general programming features than SPDL, and the potential for increased efficiency will be substantial due to SPDL's page

independence.

Efficiency in terms of storage costs and software development time should be similar to Interpress and PostScript, as well. Software development costs might actually be reduced for encoded forms, since development could occur in human-readable forms, and be translated after debugging.

4.3 How SPDL differs from the major proprietary PDLs

SPDL is a richer language in terms of structure information than the conventional PDLs. Most PDLs do not support as much document description information as SPDL. DDL is the exception, and SPDL's structure information appears to be a superset of that available with DDL. Page independence separates SPDL from all but Interpress.

SPDL has a richer imaging model than the major PDLs. SPDL's Ink plane is substantially more flexible than its competitors. Support for patterned Ink planes is a substantial departure from the past.

It is unclear if SPDL will follow the lead of DDL or conventional wisdom in terms of scalable bitmaps, but the current draft indicates that bitmap fonts will be scalable. The DDL specification details a method for scaling bitmap fonts. SPDL does not include any specific information on the method of implementing such scaling.

SPDL's support for document description is stronger than that available with Interpress, but weaker than that in DDL. SPDL will not include anything comparable to DDL's DLL and DCL faciilities (see section 3.5). The opinion of the interested standards bodies is that such information belongs in the print services protocol, and will be left to future standardization efforts.

The most important difference, though, is that SPDL will be an international standard, supported by ISO, ECMA and ANSI among others. An international standard has certain advantages over proprietary and psuedo-proprietary systems.

4.4 What SPDL will give the user that current PDLs do not

One of the main advantages that SPDL will present is based on its status as an international standard. SPDL is a more open specification than the current PDLs. The number of PDL vendors offering SPDL implementations should exceed that of PostScript or Interpress, especially if a standards making body develops a conformance strategy and a corresponding set of tests. The number of vendors offering SPDL will not be large initially, as smaller vendors will stick with their current PDLs until the market develops. The largest equipment vendors (DEC, IBM and Xerox) will provide early support for SPDL to hold onto their current market with large corporations or federal agencies.

A second advantage presented by SPDL will be the wide range of equipment that its twin encodings will cover. As a human readable encoding SPDL will be available on low-volume imaging devices. Machine encoded SPDL will appear on high-volume, high-speed imaging devices where the inefficiency of parsing a human readable PDL is currently considered to be unacceptable.

Pictures are explicitly defined in the SPDL specification. The fact that the definition and specification is enforced by the language makes this a strong base for applications with this requirement.

SPDL will have another advantage due to its extensive integration with other ISO standards. It will be integrated with the font standard, ISO 9541 (currently a Draft International Standard), ISO standards for image compression and color, and the document structure will be encoded in ASN.1 and SGML. Integration with other standards ensures maximum utility by allowing SPDL to be used with other products based on these ISO standards.

5.0 Conclusions

SPDL is substantially different from the PDLs with a measurable market share. This means that it will compete in some ways, but will often be most attractive to customers for whom no single PDL is presently able to do the job.

SPDL will prove to be of immediate interest in large organizations with requirement for a wide range of imaging devices (in terms of cost, speed and resolution) that no single PDL has previously been able to support. Organizations that have previously supported a multitude of

PDLs can adopt an SPDL migration strategy, and replace all of their PDLs with two encodings of SPDL. Since a simple software translator will translate one encoding to the other, all PDL document instances will be compatible with any imaging device. Document archives involving storage of PDL instances will become a great deal more attractive if a single PDL is available on all imaging devices.

SPDL will not prove to be a competitor in the large "mainly text" market dominated by PCL. Since SPDL is most similar to PostScript and Interpress, pricing will be similar to those machines. The discounts available in comparison to those PDLs will be based on the (expected) increase in competition among PDL vendors, since development time will be similar to those PDLs.

The area of overlap between SPDL and DDL is substantial. While this serves in many respects to validate some of the design choices made by Imagen, it also indicates that SPDL will compete directly with DDL. Imagen may find this a very difficult position, and probably will be unable to gain any substantial market share. DDL has certain features that were avoided in SPDL. This should allow SPDL printers to be faster and cheaper. SPDL is considerably more attractive to most PDL vendors than DDL. Entrenched printer vendors are more willing to support an international standard than another company's design. An international standard, with a registered conformance test body, would offer many advantages to manufacturers wishing to develop their own implementations.

References

[DDL] DDL Reference Manual Imagen Corp., 1986 400-1101 Rev. 1.

[INTE] Interpress Electronic Printing Standard Xerox Corp., January 1986 XNSS 048601.

[KNUT] Knuth, Donald The TeX Book.

[POST] PostScript Language Reference Manual Adobe Systems, Addison-Wesley 1985.

[ROSE] "Text and Graphic Standards in the CALS Publishing Environment", September 1988

[SPDL] Standard Page Description Language, 3rd Working Draft March 1988
ISO JTC1/SC 18 N 1402.

TEXT

SPDL Conformance Strategy

CALS SOW TASK 2.4.4.1

SPDL Conformance Strategy

William T. Polk
National Computer and Telecommunication Labratory
National Institute Of Standards and Technology

Introduction

This paper is designed to present a strategy for development of a validation suite for SPDL imaging systems. The paper begins by presenting a brief overview of SPDL. The overview is followed by an examination of the appropriate conformance issues. The basic architecture of an SPDL imaging system is then reviewed to determine what data is available to use in validation tests. Finally, the Summary attempts to place all the information into a reasonable perspective: what are the major problems, what can (or can't) be tested, and what is necessary for NIST/NCTL to proceed in this important project?

What is SPDL Anyway?

The Standard Page Description Language, or SPDL, is a language designed for the device independent representation of fully formatted documents. SPDL is a project of ISO/IEC JTC1/SC18 and is currently in the working draft stage. It is most obviously heir to the tradition of Interpress and PostScript, but contains ideas drawn from many other sources, as well.

SPDL is a two-tiered langauge. At the first tier, SPDL has a hierachical structure notation. This structure notation envelops a reverse polish language for the description of images (text and graphics objects). The portion of a document instance devoted to structure notation is referred to as the *wrapper*. The portions of the document instance describing images are called the *token stream*.

An SPDL document instance would usually be generated by an application. That application might be a word processor, graphics package, or electronic publishing package. The document instance would then serve as input to an SPDL Imaging System.

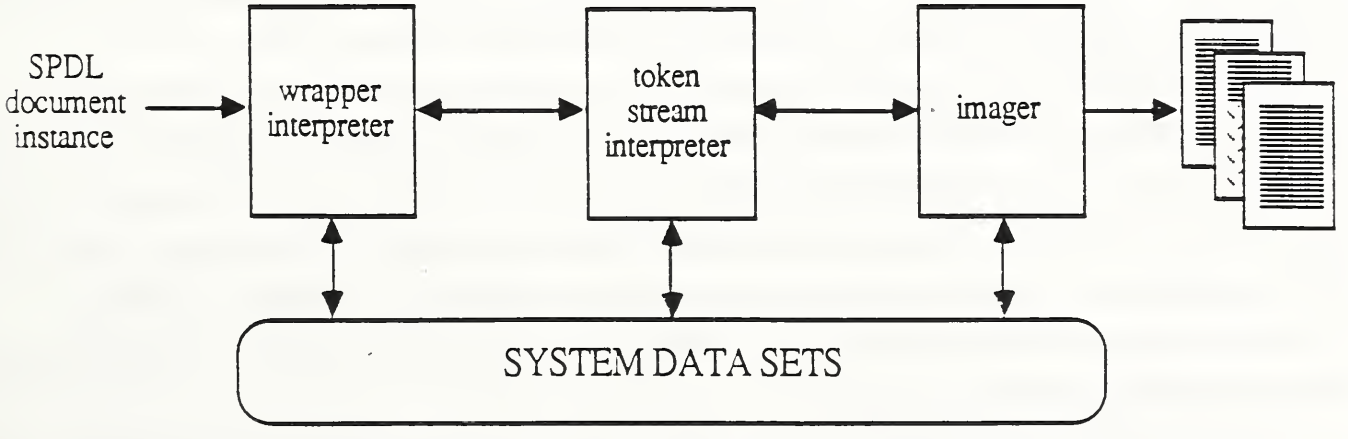


Figure 1. Overview Of An SPDL Imaging System

An SPDL Imaging System must do three basic tasks: it must interpret the wrapper to ascertain

the relationships of the images; it must interpret the token stream to see what images are being described; and it must translate the described device independent image into the best approximation possible for the physical rendering device at hand.

An SPDL Imaging System can be modeled as a series of three processing systems, one for each task, and several shared system data sets. Each system is associated with a stateless processor and several data sets. The state of that system is defined entirely by the contents of the data sets.

For SPDL to be successful, it is necessary that all SPDL devices render a single document in an "equivalent" fashion. This requirement can only be met if there is a set of objective conformance tests available so that system developers can demonstrate and validate the correctness of their implementation.

Note: SPDL has two parallel encodings. The first encoding is human readable, the other is an encoded form. (The most obvious corollary would be assembly code vs. machine code.) This is an attempt to bridge the two worlds of high-speed, high-volume printing, and low-volume desktop printing. Since the encodings are parallel, documents (and tests) are interchangeable between types of systems. Therfore, this feature can (and will) be ignored for the remainder of this paper.

SPDL Conformance Issues: What do we wish to prove?

This section is an attempt at defining the issues of concern in SPDL conformance. The paper should be correlated to the PDL technology paper. The validation tests should be correlated to this document. The basic tests should cover every function in the specification, each possible error message, and every specified side effect; i.e, do the basic functions work as they are supposed to. This is a list of questions we expect a validation suite to answer, and a note about some questions a validation suite simply can't answer.

1. *Can an SPDL system recognize if a document instance is a conforming SPDL document instance?* This is a question of syntax only. The syntax is two-fold: both the wrapper structure and token sequence must be valid. The wrapper structure has a specific grammar that must be satisfied. The token sequence is valid if each token in the token stream is valid.

[There is a corrolary to question number 1. *Is a document a conforming SPDL document?* This is important to developers whose systems will be producing SPDL document instances or SPDL pictures. I am unsure if this should be addressed. Also, note that this has a corrollary as well - "Does the SPDL document produced describe the right image?" This is not a question for SPDL conformance. Only the system developer can say if that image is what was intended.]

2. *Does the interpreter work correctly?* This question is important to SPDL imaging systems developers, and to their customers.

This leads to a large number of questions. One: do the appropriate error messages get triggered as specified?; Two: do the functions return the correct results? (i.e, do the right answers appear on the stack?) and Three: are the internal side effects correct? (Internal side effects are those

modifying the memory store, state variables, etc.) Four: does the system recognize the wrapper syntax correctly? and does it perform the correct functions in response to that wrapper structure?

3. *Does the image rendered correspond to that described by the document instance?* This question is important to SPDL imaging systems developers, and to their customers.

This is again a question of side effects. The correct answer to this question depends on several system parameters including resolution and support (or lack there of) for colour and gray scales. This test must suffice for the testing of imaging state variables, since those are NOT specified in the standard.

This is a question of "How do things look?", which is difficult for many reasons. The "look" of a document tends to be affected by the imaging technology (write-black vs. write-white vs. bitmap display vs. plotters), as well as the aforementioned parameters. Tests for the "look" tend to be subjective, but only objective tests are appropriate for inclusion in a conformance suite. It is not clear at this time how such real effects testing may be objective, or how to handle system parameters in such testing.

There are several possibilities that may be examined. The tests should probably all be relative to themselves (i.e, the answer should be determined without comparison to a "sample sheet"). It may be possible to use different tests for each group of peer systems (in terms of system parameters). This could be done with limited modification of template programs.

Note: Some things can not be tested. Some areas, such as font scaling, are considered to be areas in which products must compete. These areas are given minimal coverage in the SPDL specification. These areas are covered only to such an extent as to say that they must be supported, but without stating the end result. Therefore, they cannot be validated in terms of real effects (presented image). The only possible validation is to show such commands do not return errors.

SPDL Conformance: What Data Is Available To Be Tested?

An SPDL imaging system may be thought of as three seperate processors - a wrapper interpreter, a token stream interpreter, and an imager. The processors are actually stateless; that is, the actions of the processors are determined by the input to it, and the contents of the system data sets. How those system data contents were arrived at it is unimportant. The SPDL specification actually specifies how those data sets should be changed by the processors. While the important question is "Do the processors work?", the answer cannot be determined from the processors themselves. The information can only be determined indirectly by examining the data sets.

A functional diagram of an SPDL rendering system is shown as figure 2. The diagram has been coded to divide the parts into their corresponding types (processors and data sets). Note that parts are white, hatch marked, or shaded. The shaded boxes may be either hatch marked, or dark gray. This divides an SPDL system into three basic sets: the first is the set of *processors*; the second and third are the *data sets* maintained by the system. The two types of data sets differ in what portion of their contents is actually specified by the SPDL specification.

The members of the set of processors are shown as white boxes. The functionality of each of the three processors is specified by the SPDL specification, but the method in which they may be implemented is not addressed. Therefore, they may not be tested directly, since any number of methods might be chosen to implement them. It becomes necessary to look for assurance of conformance indirectly, through clues left by the processors in the remaining parts of the system - the data sets.

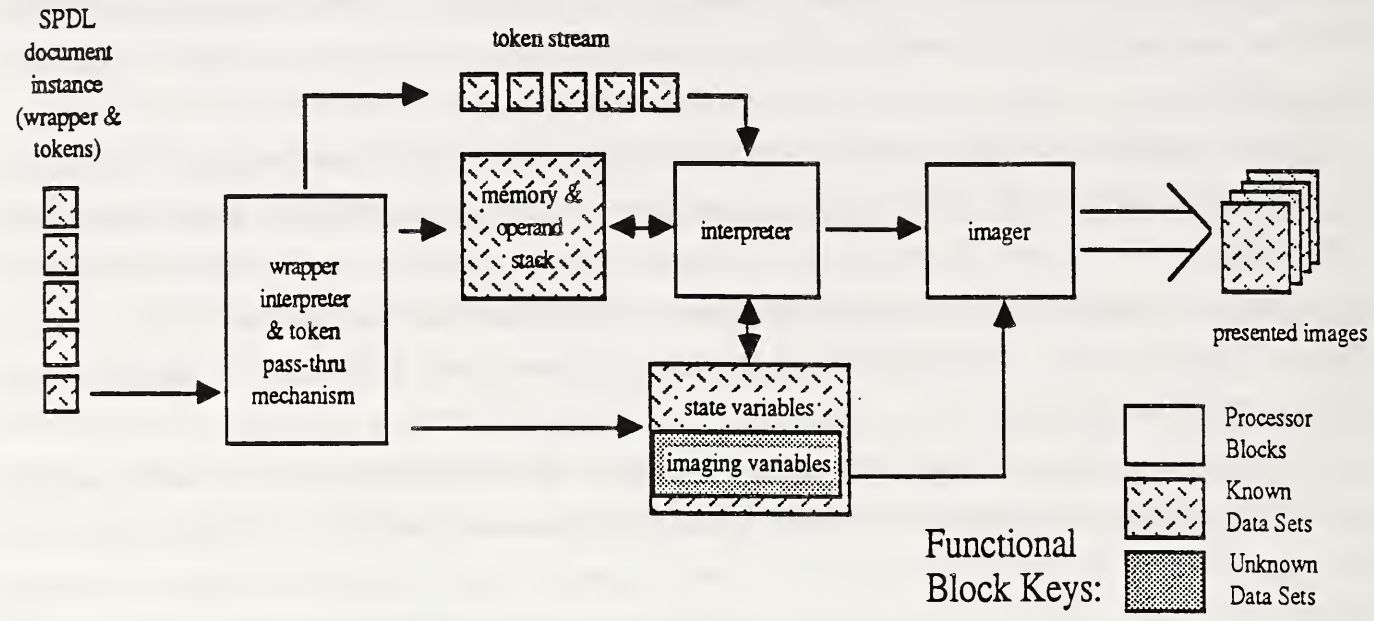


Figure 2. An SPDL Rendering System

The members of the data sets are shown as shaded boxes. The data sets may be subdivided into two more groups: *known data sets* (alternating diagonal hash marks); and *unknown data sets* (dark gray). In the case of known data sets, the correct state (i.e, contents) can be determined for any position in the token stream. (Even this is only true to a point. The SPDL specification defines all data structures. However, the system designers may implement the data structures in any method they so choose. The data structures, and their contents are known. The representation of those data structures is not.) The unknown data sets are data blocks required by the system, but unspecified in the SPDL document itself.

The validation of the processors may be performed indirectly, by examining the contents of the known data sets to verify that the expected modifications, and only the expected modifications, were made. [The second part of that statement - "only the expected modifications" - is obviously difficult to implement. It is questionable whether tests will actually be able to support that.] Note that the "known data set" includes presented images. This complicates the problem, but is unavoidable, since there are no other indicators for the imager processor functional block.

Like the processors, unknown data sets must be validated indirectly, by examining the contents of the known data sets. There is only one unknown data set in the SPDL system. This is the set of imaging variables. This set of data will be kept up to date by the imager, but is not specified in the standard. Like the imager, its contents may not be tested in any way, other than examination of

presented images.

In summary, the Wrapper Interpretation Processor and Token Stream Processor may be validated by examination of the known data sets maintained inside the system, and to a lesser extent, by examination of presented images. The Imager Processor may be validated only by use of presented images.

SPDL Conformance: A Brief Summary

SPDL conformance tests should meet several basic criteria. They must be objective, so that there is no question about the difference between success and failure. Whenever possible, the tests should be self grading. This will be of great assistance to those administering conformance tests. The real-effects testing cannot be self-graded, but should be measurable relative to itself. That is, no "reference output" should be required to determine the validity of the rendered image.

It is quite apparent that there are several dangerous pitfalls. The tests must be valid irrespective of differences in the systems, although modifications in the real effects testing may be required to take systems parameters into account. Such modifications should be kept to a minimum. Systems paremeters, such as the system's word size when testing floating point functions, must not affect the results in internal effects testing. The tests must not test areas where the SPDL standard is intentionally vague to allow vendor competition.

An SPDL validation system should consist of tests for the three main parts of an SPDL imaging system: two suites of tests to validate the internal effects of each command (one for the wrapper interpreter and a second for token stream interpreter) upon the functional blocks; and a suite of test programs to test the real effects of all the commands on the 3 functional blocks (i.e, a comparison of presented images).

We might also consider a document instance validator, which would verify that the document was syntactically correct and executed without any errors. This would essentially be a reference implementation of an SPDL imaging system.

Requirements

NIST should take a lead role in the development of conformance testing for SPDL. As a consortium of computer scientists representing major consumers (federal agencies in particular, and the business sector in general), rather than a PDL vendor, NIST is uniquely positioned to take on such work. Conformance testing is a key item for the support of a Federal Information Processing Standard (FIPS) for SPDL. Conformance testing will encourage consumers by providing some measure of guarantee that the desired interoperability will be attainable. Wi hout this assurance, there are far fewer reasons to switch to SPDL from a proprietary PDL.

The project would need to begin with SPDL development work to familiarize the staff about SPDL. This is important to the success of the project for two major reasons:

creating an SPDL implementation will assist in the formulation of an appropriate test methodology; and an SPDL implementation is critical for testing the conformance tests themselves. (As an example, the NBS reference parser for SGML was a crucial tool in the creation of the SGML validation suite. The parser pointed out errors in the test suite that the committee could not recognize.) The author firmly believes that experience in building such a system is critical to the success of any project in conformance testing.

Appropriate SPDL development projects would include SPDL forms translators (human-to-encoded and vice-versa), an SPDL to PostScript translator, and a prototype SPDL imaging system. Of these, the SPDL imaging system is the most important and most difficult. Note that the imaging system does not need to be complete. All product competition features that are not specified in the standard could be ignored, since the conformance tests will not address the issue.

Appendix A: Extending John Cugini's PHIGS Conformance Concept for SPDL

John Cugini of the National Institute of Standards and Technology has developed an ingenious concept for a test suite for PHIGS (a graphics interface supporting both two and three dimensional objects). The concept is as follows: 0) verify the result of simple (2-D) PHIGS commands; 1) simulate the result of complex (3-D) PHIGS commands with a series of simple PHIGS commands; 2) run the complex PHIGS commands to create a second image, offset from the first by some distance on the display device; and 3) compare the two images side-by-side. Serious discrepancies in the real-effects of the commands should be quite obvious.

SPDL does not support three-dimensional objects. It does, however, contain both raster and geometric graphics. John's concept might be extendable to SPDL's real-effects testing by creating bitmap images corresponding to the result of a set of commands. An SPDL instance containing both the bitmap and series of SPDL geometric graphics commands, with a change in origin between the two versions, would result in the imaging of two identical images offset by the origin change. This would allow straightforward, albeit subjective, real-effects testing.

There are advantages and disadvantages to such a method. The major advantage is that display of a bitmap is so simple that it is a fairly dependable method of checking more complex (geometric) functions. There are two disadvantages: the correct bitmap would be dependent upon the characteristics of the target device (resolution, colour, grayscale); and NIST would have to build a system to generate these bitmaps. The system used to generate the bitmaps would essentially be the prototype implementation.

SECURITY

Risk Management Tools: A Guide to Selection and Use

CALS SOW TASK 5.2

RISK MANAGEMENT TOOLS:
A GUIDE TO SELECTION AND USE

Prepared for the

COMPUTER-ASSISTED ACQUISITION AND LOGISTICS
SYSTEM (CALS) PROJECT OFFICE
DEPARTMENT OF DEFENSE

DECEMBER 1988

Prepared by

IRENE E. GILBERT

COMPUTER SECURITY DIVISION
NATIONAL COMPUTER AND TELECOMMUNICATIONS LABORATORY
NATIONAL INSTITUTE FOR STANDARDS AND TECHNOLOGY

Once appropriate safeguards have been implemented, it will be necessary to conduct periodic monitoring to ensure their continued effectiveness. Thus, the risk management process has been set into motion.

This report provides managers and others responsible for managing risks in computer and telecommunications systems with a summary of automated risk analysis tools and their applicability to the CALS security environment. A definition of concepts and terms needed to understand risk analysis and the entire risk management process is provided along with a summary of the features and characteristics of many automated risk analysis software packages. A set of criteria is provided by which to measure the capabilities of a given risk management tool.

In general, all of the risk analysis software packages introduced in this report address the security and control of automated data in any information resource management environment. While no attempt is made to perform any qualitative evaluation of the tools discussed, the risk analyst may find that certain tools may be more appropriate to various subsets of the CALS program. The integrity of CALS data and the reliability and availability of its system components are vital to the successful implementation and operation of the program. Confidentiality, availability, and access control are also important security issues that should be explored in depth by the risk management software. The selection of a suitable risk management package should be based on its ability to meet the needs of specific information environments.

In particular, the areas of user validation, data aggregation, and data/database integrity are of special concern [CALS88]. Online user access is an area that should be heavily addressed by the risk analysis package selected since access control security requirements are expected to increase as CALS includes more classified information [CALS88]. Errors, omissions, and environmental hazards are among the issues that can also impact the confidentiality, integrity, and availability of the data and other resources needed for the successful operation of CALS.

Finally, the success of a risk analysis will depend on management support and the allocation of resources to perform this vital function. Ongoing risk management efforts are required to maintain the desired level of CALS data protection.

EXECUTIVE SUMMARY

The DOD Computer-Aided Logistic Support (CALS) program is a strategy to effect a transition from current methods of acquisition and logistic support for weapon systems to an automated and integrated system of operation. The CALS program has three broad objectives:

- To accelerate the integration of reliability and maintainability design tools into contractor CAD/CAE systems.

- To encourage the automation and integration of contractor processes for generating weapon systems technical information.

- To rapidly increase DOD capabilities to receive, store, distribute, and use technical information in digital form.

The result is improved productivity and quality of information and lower life-cycle costs. The CALS implementation strategy focuses on creating an environment of distributed databases connected by local area and wide area networks that will provide DOD and industry with direct access to information they need. While this evolutionary goal of modernizing information exchange will reduce the costs of data handling and affect more timely and accurate data to users, protecting CALS data and its system components make achievement of this program a challenging goal indeed.

Several things will be essential for managing risks in the CALS environment. First, managers must understand the risks involved. Once management understands these risks, they can be managed just as other business functions are managed. The mechanism for controlling risks is an effective risk management program which encompasses risk analysis and implementation of security controls and reviews.

Risk analysis is a part of risk management that analyzes system assets and vulnerabilities to establish an expected loss from events based on estimated probabilities of occurrence. The purpose of risk analysis is to determine if the safeguards currently in place are adequate to reduce the probability of loss to an acceptable level. Moreover, risk analysis results are used in the selection of cost-effective corrective measures and safeguards. The major benefits of a risk analysis are to identify the following:

- critical software applications
- threats and threat frequencies
- vulnerabilities to threat
- consequences of the occurrence of threat
- safeguards to protect, detect, and mitigate threats
- costs of safeguards; and
- cost benefit analysis

EXECUTIVE SUMMARY

The DOD Computer-Aided Logistic Support (CALS) program is a strategy to effect a transition from current methods of acquisition and logistic support for weapon systems to an automated and integrated system of operation. The CALS program has three broad objectives:

- To accelerate the integration of reliability and maintainability design tools into contractor CAD/CAE systems.

- To encourage the automation and integration of contractor processes for generating weapon systems technical information.

- To rapidly increase DOD capabilities to receive, store, distribute, and use technical information in digital form.

The result is improved productivity and quality of information and lower life-cycle costs. The CALS implementation strategy focuses on creating an environment of distributed databases connected by local area and wide area networks that will provide DOD and industry with direct access to information they need. While this evolutionary goal of modernizing information exchange will reduce the costs of data handling and affect more timely and accurate data to users, protecting CALS data and its system components make achievement of this program a challenging goal indeed.

Several things will be essential for managing risks in the CALS environment. First, managers must understand the risks involved. Once management understands these risks, they can be managed just as other business functions are managed. The mechanism for controlling risks is an effective risk management program which encompasses risk analysis and implementation of security controls and reviews.

Risk analysis is a part of risk management that analyzes system assets and vulnerabilities to establish an expected loss from events based on estimated probabilities of occurrence. The purpose of risk analysis is to determine if the safeguards currently in place are adequate to reduce the probability of loss to an acceptable level. Moreover, risk analysis results are used in the selection of cost-effective corrective measures and safeguards. The major benefits of a risk analysis are to identify the following:

- critical software applications
- threats and threat frequencies
- vulnerabilities to threat
- consequences of the occurrence of threat
- safeguards to protect, detect, and mitigate threats
- costs of safeguards; and
- cost benefit analysis

1. INTRODUCTION

The Computer-Aided Acquisition and Logistic Support (CALS) program is a DOD strategy by which the Department of Defense (DOD) will automate weapon system technical information over the system's life-cycle. With the potential for interactive access to weapon system data, appropriate computer security controls and risk management must be put into place to ensure data protection and security.

Risk management involves the entire spectrum of technology, procedures, and practices that provide protective measures necessary to ensure the confidentiality, integrity and availability of vital computer resources, notably information. Risk analysis sets the stage for the entire risk management process. It is a process periodically undertaken to identify security risks and to select safeguards. Risk analysis provides a yardstick for determining the amount of money which is reasonable to spend on each safeguard. Risk analysis identifies not only critical information and data but considers the system components and the environment in which the information is stored and processed.

Specifically, risk analysis performs the following functions:

- identify existence of undesirable events (threats);
- assess weaknesses in the system (vulnerabilities);
- determine the effect on systems, facilities, and operations (impact);
- assess the cost of potential loss (loss exposure); and
- assist managers in the selection of cost-effective safeguards.

When the risk analysis has been completed, the risk manager will have a clear picture of significant threats and what safeguards are necessary to protect the organization's assets. Safeguards may act in several ways:

- reduce the likelihood of the occurrence of threat
- reduce the impact of threat occurrences
- facilitate recovery from threat occurrences

When selecting safeguards the greatest emphasis should be placed on areas of greatest potential loss or harm. The second criteria is that they [safeguards] be cost-effective. The costs should relate to the losses against which they provide protection. In other words, the safeguard should return more in savings than it costs.

This next point may seem obvious, but it is not uncommon for a manager to select a safeguard without first doing a risk

analysis. The result may be a serious over-expenditure of funds for protective measures. Even worse, the implemented safeguards may not do an adequate job of reducing the actual (undefined) risks. It would be more prudent for the manager to factor his judgement into a risk analysis [FIPS31].

The point to be made here is that risk analysis is the basis for establishing a cost-effective risk management program and ensuring that reasonable steps have been taken to prevent situations which can interfere with accomplishing the mission.

1.1 PURPOSE AND SCOPE

The purpose of this document is to describe various methods for analyzing computer and information security risks in the CALS environment. The report addresses the issue of selecting automated risk analysis tools for the CALS security environment and emphasizes the need for managers to support the planning, funding, and implementation of cost-effective safeguards based on the results of a risk analysis. This document fulfills the requirements of the CALS 1988 Statement of Work, Task 5.2.

1.2 OVERVIEW OF DOCUMENT

Section 2 provides information on the Federal government's activities in formalizing the risk management process. A discussion of concepts and terms needed to understand risk management is also provided in this section.

A presentation is made in Section 3 of the general characteristics of risk analytic software tools currently available, along with a discussion of their advantages and disadvantages. Section 4 provides a set of generic requirements criteria by which to measure the appropriateness of any given tool. Risk analysts should develop their own site-specific requirements for each of the criteria discussed in order to evaluate the suitability of a variety of risk management software packages.

Section 5 provides a summary of the capabilities and characteristics of available packages. Appendix A provides the characteristics of specific packages, and Appendix B contains a list of additional references.

2. BACKGROUND

2.1 RISK MANAGEMENT ACTIVITIES IN THE FEDERAL GOVERNMENT

The National Institute of Standards and Technology (NIST, formerly National Bureau of Standards) has produced many publications including the Federal Information Processing Standard (FIPS), Guideline for Automatic Data Processing Risk Analysis [FIPS 65]. FIPS 65 represents the first attempt by the Federal government to formalize the risk management process in computer environments. This document was prepared for the purpose of providing a technique for doing risk analysis in Federal agencies. It was developed with the understanding that risk analysis technology was still in its evolutionary phase and that continued research was necessary for developing more sophisticated and more easily applied techniques. Research has continued in both the private and Federal sectors, and since the time FIPS 65 was issued a variety of approaches for doing risk management have become available.

While there are a variety of risk analysis software packages available, questions remain as to whether these packages are complete or accurate. In recent years the NIST has expanded its activities in the risk management area to build its experience base and to obtain hands on experience with current methods and to develop criteria for comparing different approaches. NIST and the National Computer Security Center (NCSC) have agreed to assume a leadership role in improving the state of the art in the risk management area. Cooperative arrangements with several developers of automated risk management software has led to the review of some of these packages in the NIST/NCSC Risk Management Laboratory [KATZ88].

In addition to the joint effort with NCSC, NIST will continue to work with Federal agencies and the private sector by providing assistance with their risk management activities and by engaging in research and development efforts that lead to practical approaches to risk management which responsive to a broad class of computer security environments.

2.2 CONCEPTS AND TERMS

INFORMATION SECURITY OBJECTIVES

Before discussing specific considerations for selecting a risk management tool, it will be useful to define the basic concepts and terms needed to understand information security objectives and the risk management process.

First, it should be recognized that no matter what the size or nature of an ADP system or application, the following major security objectives must be met:

- o Confidentiality of personal, proprietary, or otherwise sensitive data handled by the system.

- o Integrity and accuracy of data and the processes that handle the data.

- o Availability of systems and the data or services they support.

If these objectives are met, then other assets that are dependent on the information being protected will also be protected.

ANNUAL LOSS EXPECTANCY (ALE)

Annual loss expectancy is the projected loss (in dollars) that one can expect with a computer system in a year.

RISK MANAGEMENT

Risk management involves the entire spectrum of technology, procedures, and practices that provide protective measures necessary to ensure the confidentiality, integrity and availability of vital informational assets.

RISK ANALYSIS

Risk analysis is a procedure used to estimate potential losses due to system safeguard vulnerabilities. Risk analysis serves to point out the risks that exist within an organization and the damage which can result from undesirable events. The ultimate purpose of risk analysis is to help in the selection of cost-effective safeguards that reduce risks to a level acceptable to management.

ASSETS

System assets are the central feature of the risk analysis process. The risk analysis methodology should allow the risk analyst to define exactly what they are trying to protect and its value. In the past, risk assessments concentrated on the physical hardware components. In recent years, consideration for the cost of replacing software, data, and documentation has become important.

SENSITIVE INFORMATION

Sensitive information means any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (the Privacy Act), but which

has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy [COMP87].

VULNERABILITIES

Vulnerabilities are weaknesses in the safeguard's system intended to protect the organization's assets.

THREATS

A threat is a person, thing, event, or idea which poses some danger to an asset. A threat may compromise the confidentiality, integrity, or availability of an asset by exploiting vulnerabilities or weakness in the system. Threats may include both unintentional acts as well intentional, such as sabotage. There are many other common threats that can effect an organizations day to day operations. These common threats include the following:

- errors and omissions
- failure to backup critical data files
- improper handling of magnetic media
- disclosure of proprietary information
- unauthorized use of hardware and software
- theft of equipment
- violation of software licensing agreements
- power interruptions
- environmental failures

SAFEGUARDS

Safeguards are individual physical controls, mechanisms, policies and procedures that protect assets from threats. Examples of safeguards are fences, alarms, guards, sprinklers, passwords, access controls, policy statements, offsite storage, contingency plans, tempest shielding, and so forth. In order for a threat to occur, one or more of the safeguards must be bypassed or circumvented entirely or in part.

SAFEGUARDS SYSTEM

A safeguards system is the complete collection of all safeguards. The ability to identify countermeasures or safeguards system that will reduce vulnerabilities and thereby the risks is an essential component of risk management. A risk summary in either text or graphic representation of various safeguard alternatives with their cost benefit tradeoffs along with a prioritized list of recommended safeguards provides a comprehensive analysis.

SAFEGUARD COST/BENEFIT ANALYSIS

Security expenditures should be cost-justified just like every other expenditure an organization makes. Thus, the key to the selection of optimum security measures is the ability to estimate the impact of a proposed or existing security control on future losses. A safeguard cost/benefit analysis enables the manager to easily develop costs associated with the acquisition of each safeguard over the projected life of the safeguard. The cost of security measures should compare favorably with the reduction of expected future losses.

LIKELIHOOD OF OCCURRENCE

Likelihood of occurrence is a measure of the possibility of something happening or of something that exists. An ability to analyze the likelihood and severity of a threat can provide an assessment of the overall risk of compromise to system assets.

OUTCOME

An outcome refers to the undesirable result of a threat's action against the asset which results in measurable loss to the organization.

RESPONSIBILITIES IN THE RISK MANAGEMENT PROGRAM

Generally, the risk management process provides a greater awareness among the staff to strengthen their risk management program. In the past, the responsibility of managing risks was that of the ADP Manager. This approach has changed, and now many groups within an organization share the responsibility for a successful risk management program.

1. The risk analyst is responsible for gathering and processing the input information. The analyst has further responsibility for presenting to senior management the best possible information for safeguard selection.

2. Users are responsible for providing accurate information about their applications to the risk analyst. Additional information from other support functions such as Building Engineering, Personnel, Physical Security, etc., are responsible for providing input data about environmental and outside threats.

3. ADP Operations staff are responsible for providing information about the hardware, software, and procedural functions.

4. Senior Management has responsibility for the initial

support and funding of the risk management program and is ultimately responsible for ensuring the protection of organizational assets. Specifically, senior management should do the following:

- Demonstrate to all levels of the organization a firm commitment to planning and supporting a risk management program.
- Assign responsibility to manage the risk management program.
- Commit the resources necessary to conduct risk analysis and carry out the risk management program.

3. AUTOMATED RISK ANALYSIS SOFTWARE PACKAGES

3.1 GENERAL FEATURES AND CAPABILITIES

Many techniques are used to measure and evaluate risks in computer systems, yet all can be categorized as either quantitative or qualitative [MAY88]. The methodologies used in the risk analysis software presented in this report accomplishes three basic steps:

- o asset identification
- o risk calculation
- o safeguard evaluation

The asset identification phase is generally accepted as the most important step in the risk management process for it provides management an awareness of the need for security, or it may point out that there is nothing of substantial value in the application under review that needs protecting. Each of the software packages evaluate tangible assets, such as facilities and material, and intangible assets, such as organizational reputation and employee motivation and morale. Each of the packages consider the cost of replacing software, data, and documentation as well as physical and environmental security controls.

Some of the risk management packages presented here use the traditional approach for calculating risks, as described in FIPS Publication 65. Using this approach, threats are considered in terms of the estimated costs associated with their impact and the frequency of occurrence. These estimates are expressed in terms of orders of magnitude, hence a quantified set of values is specified for both the impact and the frequency. Other packages that use the qualitative approach express risks with scalar values. Still other risk management methodologies claim to be "expert systems" with security intelligence built into them to derive a body of both facts and speculative data.

The next phase of the risk analysis software considers the various security safeguards (or countermeasures) available. Some software packages consider their associated costs as well. The benefit of cost considerations is estimated from the difference between the loss impact and the cost of the security safeguard.

Currently, only one automated risk management software package processes on a mainframe, while others process on microcomputers. Most make use of questionnaires and menus. Some produce results expressed in precise quantitative, economic terms while others make use of qualitative expressions or approximations.

3.2 QUANTITATIVE APPROACH

Quantitative analysis provide a dollar loss measure of risk and an estimation of the frequency with which an adverse event may occur. Some risk management methodologies use annualized expected loss (ALE) algorithms which averages the value of future losses based on an estimated occurrence rate of threats associated with an asset, while others calculate single occurrence losses. A single occurrence loss (SOL) is the estimate of the loss which occurs from a single occurrence of a threat and does not depend upon the rate of occurrence.

3.3 QUALITATIVE APPROACH

The qualitative approach takes the point of view that many potential losses are intangible, and therefore risks cannot be readily specified monetarily. The risk results are portrayed in a linguistic manner (i.e., "no risk" to "very high risks"). Some qualitative approaches carry the risk result a step further, where risk is represented mathematically as a scalar value (i.e., a value from one to five) with descriptive terminology for each point on the scale.

3.4 ADVANTAGES AND DISADVANTAGES OF USING AUTOMATED PACKAGES

Clearly there are benefits and limitations to any of the current risk management methodologies. It is only when site-specific criteria are established that a "preferred" methodology can be selected. Following is a discussion of some of the advantages and disadvantages of using automated risk management software packages.

3.4.1 ADVANTAGES

Unlike manual analysis that usually take months to complete, the automated methodology can discover system weaknesses in a much shorter time frame. The analysis can be carried out quickly enough to ensure that the results are not outdated by changes in the system.

Further, automated risk management software packages are easily adaptable to operational and administrative systems of all sizes, and generally allow the user to quickly explore the results of implementing certain safeguards. Some of the packages are suitable for use during the development of a system as well as for the analysis of existing systems.

3.4.2 DISADVANTAGES

One major problem is that are is no standard method or agreed upon approach for performing risk analysis, and there is no assurance that any particular method is complete or accurate. This can make it difficult for users to select the best risk management tool for their needs. The root questions in analyzing risk management software tools must be, "What is the tool measuring, and are the results useful?"

4. SELECTION CRITERIA

This section provides a set of generic requirements criteria and other issues that must be considered when evaluating risk analysis software. Risk analysts should develop their own site-specific requirements for each of the generic requirements discussed in Section 4.2 in order to evaluate the suitability of the software described. Such an evaluation will help to ensure that the most appropriate software is selected. The requirements criteria discussed include:

- o Hardware compatibility
- o Methodology
- o Reports
- o Documentation
- o Audit trails
- o Training
- o Cost

Further, any risk analysis tool, whether it is used to analyze a computer facility or an application should satisfy the principles described in Section 4.1.

4.1 INPUT PHASE

The software must have a structure for gathering information either textually or graphically about the system under study. Information should be gathered about the organization's mission, assets and their valuation, environment, potential threats, and safeguard systems or controls already in place.

4.1.1 Asset Identification

The asset identification phase is necessary to identify resources that are to be protected and their value. The software should provide an approach for developing an asset-inventory for all assets and their replacement costs. This step, even if it goes no further, is important as it alerts managers of the need to protect organizational assets.

Assets may be categorized as tangible and intangible. Following is a list of tangible assets:

- o Facilities
- o Hardware
- o Software
- o Supplies
- o Documentation
- o Personnel
- o Data

Intangible assets may include the following:

- o Replacement cost
- o Denial of use cost
- o Misuse and abuse
- o Goodwill

The manner in which safeguards are selected will depend greatly upon the intended function of these assets and their value. In civilian government agencies, availability and integrity of assets may be of primary concern, while in Defense, confidentiality may play a greater role.

4.1.2 Mission

Information gathered about the organization's mission determines the level of protection the safeguards must achieve to protect informational assets.

4.1.3 Environment

Many factors will contribute to the organizations environment and each factor should be addressed in the information gathering stage of the risk analysis process. Those environmental factors that generally have an effect upon the analysis include geographic location, community, physical, and procedural controls. Geographical location determines to a large extent the potential for environmental hazards (i.e., hurricanes, earthquakes, severe thunderstorms, etc.) Information gathered about the organization's community environment will describe the social, political, and intellectual character. Procedural controls usually characterize the policy and procedures of the organization.

4.1.4 Safeguards, Threats/Vulnerabilities

Information should be gathered about the organization's safeguards and the vulnerabilities that each safeguard will act to mitigate. Information should be gathered about current threats, both internal and external. There are five safeguard/threat/vulnerability categories:

- o Administrative security
- o Physical facilities security
- o Access security
- o Software security
- o Hardware security

A discussion of other criteria that should be used to select an appropriate risk management methodology follows.

4.2 REQUIREMENTS DEFINITION

4.2.1 HARDWARE COMPATIBILITY

It will be cost-beneficial that the risk analysis software process on computer hardware commonly in place at the organization rather than procuring special computers. Peripheral requirements must be specified such as a requirement for a color monitor, graphics capabilities, plotter, or modem. An organization's inability to meet any of these requirements should result in immediate disregard for the software.

4.2.2 METHODOLOGY

If a requirement for a particular methodology (e.g., quantitative or qualitative) has been established, then the software must satisfy this requirement.

4.2.3 OUTPUT PHASE

Output reports will vary. At the very least, the output should present a summary of risks and provide the user with safeguard alternatives along with their cost/benefit analysis. A prioritized listing of recommended safeguards based on the mandatory security requirements and their expected savings in loss reduction while not mandatory is a desirable feature.

4.2.4 SUPPORTING DOCUMENTATION

Documentation associated with the software is essential. The documentation is expected to provide information that will explain the operation of the risk management application software, instructions for loading, explanations of error messages, and instructions for re-execution.

4.2.5 AUDIT TRAILS

It will be a desirable feature to have audit capability since the information provided is considered sensitive as it points out the vulnerabilities of the organization. At a minimum, the audit capability if available should provide the following information:

- Identification of system software users
- Date of entry
- Data modifications, additions and deletions

4.2.6 TRAINING

Effective use of any risk management software tool depends in part on the training of the risk analysts who will use it.

Therefore detailed guidance and training should be provided as an integral part of the software purchase.

4.2.7 COST

It will be important to understand all fees involved, such as the cost of multiple copies of the software, training, and installation costs. However, cost alone should not dictate the choice of a risk analysis software package. All of the requirements necessary to conduct a risk analysis should be weighed when evaluating a package.

5. PRODUCTS SUMMARY

The first automated risk analysis package in the early 1980s ran on an IBM mainframe computer. Since then, all other risk analysis packages run on IBM or compatible microcomputers. These products represent a trend in the market because they allow risk analyses to be done independently of the mainframe computer center. The following is a discussion of the general characteristics and attributes of available risk management software.

5.1 DATA COLLECTION PHASE

The automated risk analysis software products include a detailed data collection capability. A set of programs will then calculate the information into a comparative analysis which is used to determine which safeguards are necessary. It is only when a large body of information has been collected for specific threats that honest results be forecasted.

5.2 ANALYSIS PHASE

The risk management software will analyze the information gathered to determine the potential impact or loss exposure that may result from the occurrence of threats. Analysis of each of the four major risk analysis components (assets, threats, vulnerabilities and safeguards) will vary. The techniques used will generally fall into three groups:

1. those that use mathematical functions to express relationships between these components;

2. those that group the components into related sets for subjective analysis; and,

3. those that attempt to heuristically derive scenarios or consensus feelings about risk [MAY88].

5.3 SAFEGUARD SELECTION PHASE

Some risk analysis packages make specific recommendations for safeguard selections while others simply inform the user that a vulnerability exists and make no recommendations for corrective action. Nonetheless, once the information has been collected and analyzed, the results should be put to work to reduce those risks. The most practical approach for managing risks is to work on the risks that are the most likely to occur and those which are the most controllable. The risk analysis process should help managers to do this. First, threats should be prioritized according to the following factors:

- o Potential frequency
- o Potential loss impact
- o Ease and cost of safeguard implementation

5.4 PROCESSOR

Currently only one product requires an IBM mainframe, all others require an IBM or compatible microcomputer.

5.5 OPERATING SYSTEM

All of the risk management software packages operate on IBM PC-compatible personal computers running under the MS-DOS operating system.

5.6 SYSTEM REQUIREMENTS

Each software package has its own memory and disk requirements. Memory requirements range from 64K bytes of memory to 256KB of RAM memory. Most require a hard disk for storage of programs and data.

5.7 SOURCE CODE

The source code ordinarily is not available; however, some vendors will allow sites to tailor the product to meet special needs.

5.8 SOURCE LANGUAGE

Risk management software is written in a number of programming languages, but this generally is not important to the user since source code is not provided.

5.9 SUPPORT AND TRAINING

Technical support and training are generally available. Some vendors include training with purchase; others provide support via telephone; still others charge a fee to provide onsite training to a predetermined number of students. The amount of support provided in some cases depends upon the type of license purchased. Some vendors provide consulting services at an additional fee.

5.10 TYPES OF OUTPUT REPORTS

The types of reports produced by each of the software packages varies. Some packages produce asset inventory lists, threats/vulnerabilities checklists, ALE worksheets, safeguards selection worksheets, costs benefit analysis, tables and questionnaires included in the software. Some packages provide

the capability for the user to select, and in some cases to modify, specific reports from a variety produced.

5.11 COST

There are several basic cost elements associated with automated risk analysis software packages. It will be important to understand all of the fees involved, such as:

- o license fee
- o maintenance and installation fees
- o software updates
- o training fees

Costs alone should not dictate the choice of an automated risk analysis software package. The risk analysis methodology, types of reports, quality of documentation, and support and services offered by the vendor should be weighed.

Appendix A provides detailed characteristics for a number of risk analysis packages.

6. CONCLUSIONS AND RECOMMENDATIONS

The objective of every risk management program is to have a favorable influence on future losses. Risk analysis software tools focus on helping the analyst estimate future losses associated with automated information systems and to identify safeguards appropriate to mitigate the losses associated with such risks. Risk analyses are most useful when applied within the system development life cycle although they may be used to estimate risks to operational systems. In general, the evaluation and selection of a risk analysis tool will depend upon its ability to explore a wide variety of issues and problems and to recommend appropriate safeguards.

Although there is a variety of automated risk management tools available, the science of risk analysis for computer environments is still very imprecise, and the technology is still evolving. Consequently, a "preferred" methodology for the CALS environment is one that simply meets organizational requirements. Despite the potential problem of selecting the best risk management tool, managers should consider the answers to two fundamental questions,

- Are the salient features of the environment and system captured in the analysis?
- Are the results useful?

The final point to be made is that the performance of risk analysis alone will not provide an effective risk management program. An effective program requires that appropriate safeguards be implemented and that the organization continue to audit and review the security program to ensure continued effectiveness and appropriateness of controls. By evaluating changes in agency mission, local environment, and hardware and software configurations, managers can determine what changes should be made in the risk management program to keep it effective.

APPENDIX A

CHARACTERISTICS OF INDIVIDUAL RISK MANAGEMENT SOFTWARE PACKAGES

Application Control Matrix

Methodology. Matrix approach. This methodology presents application controls, control objectives, and risks in a matrix format. The matrix provides a summary of the security environment which allows the user and auditor to quickly view where added safeguards are needed. A data base of controls from which to make selections is included in this software package.

Hardware Requirements.

- IBM PC or compatible.
- Two diskette drives or one diskette drive and a fixed drive.

Operating System.

- MS-DOS Version 2.0 or later.

User Interface/Ease of Use.

- Menu-driven.
- Online HELP facility.

Documentation and Training.

- User Manual.

Developer/Vendor. Nander Brown & Co., Reston, VA; (202) 653-6646.

Remarks.

Government agencies may obtain copies of this software at no charge.

BDSS (Bayesian Decision Support System).

Methodology. Quantitative. BDSS is an 'expert system' programmed to ask questions that assess potential risks using quantitative data bases provided by the vendor. The user can include site-specific threat experiences which the algorithms will process. This system ranks threats and safeguards so that the representation of exposure to loss may be examined with or without controls. The analysis results are typically displayed graphically with risk curves that represent dollar loss values and probability loss coordinates. The central algorithms of BDSS are based on Bayesian statistical methods. The system produces a variety of printed reports as well as ASCII files that may be exported to the user's word processor.

Hardware requirements.

- IBM PC/AT or compatible.
- 640KB memory.
- 20MB fixed drive and one diskette drive.

Operating System.

- MS-DOS Version 3.0 or later.

User Interface/Ease of Use.

- Menu driven.

Documentation and Training:

- User manual.
- Training is not included with purchase but may be provided upon request.

Developer/Vendor. Ozier, Perry & Associates, San Francisco, CA; (415) 989-9092

Remarks.

BUDDY SYSTEM

Methodology. Qualitative. The Buddy System is an automated risk analysis methodology for microcomputers environments and comprises two components: (1) countermeasures survey and (2) security analysis and management (SAM). This software package assesses the safeguards already in place against the level of information being processed to determine whether or not the system is within an acceptable vulnerability range. Recommendations for corrective action are provided for each vulnerability that falls outside of the acceptable range. A data base containing over 100 safeguards is included in this software package. The analyst may execute "what if" scenarios" using the recommended safeguards to adjust vulnerability levels. Further, a data base query system allows the user to track recommended safeguard implementations for follow-up action.

Hardware Requirements.

- IBM PC or compatible.
- 256KB memory.
- 10MB fixed drive and one 360K diskette drive.

Operating system.

- MS-DOS Version 2.0 or later.

User Interface/Ease of Use.

- On-line HELP facility.

Documentation and Training.

- User manual.
- One-day on-site training course.
- Training component built into the software to increase security awareness.

Developer/Vendor: Countermeasures, Inc., Hollywood, MD; (301) 363-5166.

Remarks.

CONTROL MATRIX METHODOLOGY FOR MICROCOMPUTERS

Methodology. Matrix approach. This software provides a matrix approach for designing controls into microcomputer system environments. It identifies which controls are necessary to ensure adequate security in business or scientific systems. The software package contains four separate systems.

Package 1 (Designing Controls into Computerized Systems) is an educational tool that teaches the user how to design and develop a control matrix.

Package 2 (Risk Ranking the Matrix) teaches the use of Delphi and Comparison Risk Ranking techniques to rank threats and their controls.

Package 3 (Automated PC-Based Control Matrix Design) is a control matrix development package that contains a database of controls plus separate databases of threats and computer system components. This package allows one to draw a draft matrix, search the controls database and move relevant controls to a matrix controls list.

Package 4 (Show Text Presentation Graphics) is used to draw the final matrix resequencing threats, components, and controls.

Hardware Requirements.

- IBM PC or compatible or IBM Personal System/2.
- 384KB memory.
- Two diskette drives or 10MB fixed disk.
- Graphics capability.

Operating system.

- MS-DOS Version 2.0 or later.

User Interface/Ease of Use.

- A demo diskette provides a ten minute introduction to the matrix concept of designing controls into computerized systems.

Documentation and Training.

- User manual.
- Automated course.
- One or two day on-site training upon request.

Developer/Vendor. Jerry Fitzgerald & Associates, Redwood City, CA; (415) 591-5676

Remarks.

CRAMM (CCTA Risk Analysis and Management Methodology)

Methodology: Qualitative. CRAMM is a formalized security risk analysis and management methodology developed by the British government. CRAMM is composed of three stages each supported by questionnaires and guidelines. Stage 1 performs a valuation of data, information, and physical assets by considering the cost of replacing or reconstructing these assets. A qualitative value of the data on a scale of 1 to 10 is developed for the impact of disclosure, modification, availability, and destruction. the physical assets comprising the system. The information derived from this step forms the basis for a more detailed review of the systems that require more than baseline security. Stage 2 assesses the threats and vulnerabilities of each asset group and ranks the threat/vulnerability on a scale of 1 to 5, where 5 reflects a worst-case scenario. Stage 3 is concerned with identifying and selecting appropriate safeguards. To aid management in deciding upon the final selection of safeguards, this automated support tool provides a facility to explore 'what-if' scenarios.

The CRAMM software also provides a password system to reduce the risk of unauthorized access to the data that is being analyzed. Sensitivity markings are provided on all screens and hardcopy output.

Hardware Requirements.

- IBM PC or compatible.
- 640KB memory.
- 20MB fixed drive.

Operating System.

- MS-DOS 2.0 or later.

User Interface/Ease of Use.

- Menu-driven.
- On-line HELP facility.

Documentation and Training.

- User manual.
- Training available upon request.

Developer/Vendor. Central Computer and Telecommunications Agency, London, England; 011-44-1-216-3220.

Remarks.

CRITI-CALC

Methodology: Quantitative. This product uses the concept of annualized loss expectancy (ALE) to quantify the criticality of risk exposure for applications. The software collects information about each application's loss potential, optimum off-site recovery, cost of backup, cost to recover. It uses this information to calculate each application's annualized risk potential. The criticality of each application is determined by the potential for loss caused by a processing interruption and a profile of up to 14 delay factors. The user interacts with the system by means of screens which display information about the risk exposure. Once the user has reviewed the initial results, "what if" analysis may be performed by modifying the input data as a way of verifying the effectiveness of certain safeguards. The information contained in the output reports may be used to optimize contingency plans.

Hardware requirements:

- IBM PC/XT or compatible.
- 640K memory.
- 360K diskette drive.
- Fixed drive not necessary but convenient.

Operating System:

- MS-DOS Version 2.11 or later.

User Interface/Ease of Use:

- Menu-driven.

Documentation and Training:

- User manual.
- On-site training.

Developer/Vendor: International Security Technology, Reston, VA; (603) 461-0885

Remarks.

Methodology. Qualitative. GRA/SYS is a tool designed to assist internal auditors and security personnel in developing a work prioritization plan for reviewing organizational risks. Specifically, the software prepares an applications and computer activity inventory, determines the number of risks for several major control areas. A risk score that reflects the measure of risk to the organization is calculated and prioritized in descending order on a scale of 1 to 9, with 9 representing a worst-case situation. An additional report that reflects the number of times each risk occurs is also prepared. Using the output reports from this software package, the user is able to identify those risks where more effective safeguards are needed.

Hardware Requirements.

- IBM PC or compatible.
- 64KB memory.
- One diskette drive.

Software Requirements.

- MS-DOS Version 2.0 or later.

User Interface/Ease of Use.

- Menu-driven.

Documentation and Training.

- User manual.
- Training is not offered with the purchase.

Developer/Vendor. Nander Brown & Co., Reston, VA.; (202) 653-6646.

Remarks.

Government organizations may obtain this software at no cost.

IST/RAMP (International Security Technology/Risk Analysis Management Program)

Methodology. Quantitative and Qualitative. IST/RAMP is a mainframe-resident risk analysis program with an input module that is PC-resident. The software calculates the annualized loss expectancy and as well as a single occurrence loss. The system can also provide a qualitative analysis. IST/RAMP generates data collection forms to assist the risk analyst in organizing and controlling data collection. Five loss categories are addressed: service interruptions; physical loss and damage; fraud; unauthorized disclosure; and errors and omissions. A library of data bases enables the analyst to maintain an audit trail of input data changes. A 'what-if' capability enables the analyst to select the most cost-effective security measures.

RAMP<->LINK is a PC-resident, menu-driven data entry system which uses risk information entered by the analyst to build a DOS file that can be uploaded to IST/RAMP for processing.

Hardware Requirements.

- IBM Mainframe for IST/RAMP.

- IBM PC/XT or compatible for RAMP<->Link.
- 512K memory.
- Two diskette drives or one diskette and fixed disk drives.

Software Requirements.

- MS DOS Version 2.1 or later.

User Interface/Ease of Use.

- Menu-driven.

Documentation and Training.

- User manual
- Three-day on-site training.

Developer/Vendor. International Security Technology, Reston, VA., (603) 461-0885.

Remarks.

RAMP<->LINK makes it unnecessary for the analyst to be familiar with the details of IST/RAMP data entry formats. The analyst enters the data off-line and logs onto a mainframe where IST/RAMP is resident using any communications software package that has a "file send" command.

JANBER

Methodology: Qualitative. Janber initiates a yes/no questionnaire and checklist for collecting information about security controls already in place. The software weights safeguards currently in place and measures them against the level of data being processed on the system. These data classification levels point to highly sensitive but unclassified information to highly classified data. The analysis provides a linguistic characterization of the level of vulnerability from 2-28, with 28 representing a worst-case scenario. Vulnerabilities, safeguards and their weights can be preestablished by the vendor to meet the organization's requirements. Safeguards that are required but not implemented are flagged in a report and recommendations for safeguards that meet organizational guidelines and directives are provided. Users have the capability of performing "what-if" scenarios to evaluate the effectiveness of certain safeguards.

A data base query system that allows the user to track recommended safeguard implementations for follow-up action is provided. Information, such as inventory data, are helpful in developing contingency plans.

Hardware Requirements.

- IBM PC or compatible.
- 10MB fixed drive and one diskette drive.

Operating system.

- MS-DOS Version 2.0 or higher.

User Interface/Ease of Use.

- Menu-driven.

Documentation and Training.

- User manual.
- Training provided upon request.

Developer/Vendor. Eagan, McAllister ASsociates, Inc., Lexington Park, MD 20653; (301) 862-3565.

Remarks.

LRAM (Livermore Risk Analysis Methodology)

Methodology: Quantitative. A government-developed system, this methodology is structured to allow screening of asset/threat-event combinations so that only high impact risks are reviewed. The methodology focuses attention on the effectiveness of proposed security controls as well as those already in place. LRAM is divided into three major phases to include project planning, risk analysis, and decision support. The initial phase defines the scope of the analysis and identifies needed resources and personnel. The second phase collects and analyzes the data collected from phase 1. In this second phase, risk elements are identified by establishing corresponding threats, control and asset components, the results of which are provided as input for the final decision support phase. The final phase presents cost-benefit estimates for each proposed safeguard along with a prioritization and selection scheme.

Hardware Requirements.

- IBM PC or compatible.
- 640K memory.
- One diskette drive and fixed drive.

Operating System.

- MS-DOS Version 2.0 or later.

User Interface/Ease of Use.

- Menu-driven.

Documentation and Training.

- User manual.

Developer/Vendor. Lawrence Livermore National Laboratory, Livermore, CA; (301) 459-0601.

Remarks.

LAVA (Los Alamos Vulnerability and Risk Assessment)

Methodology: Qualitative and Quantitative. LAVA administers questionnaires which results in the identification of missing safeguards in 34 areas ranging from password management to personnel security and internal audit practices. The software evaluates potential consequences and impact upon the organization and the ultimate loss exposure (risks). LAVA considers two kinds of threats: natural and environmental hazards, and accidental and intentional human threats. Detailed reports provide a qualitative analysis of the risks identified. LAVA provides a capability to translate the results into quantitative terms where appropriate.

Hardware requirements.

- IBM PC/XT or compatible.
- 512KB memory.
- 360KB and 720KB diskette drives; or 1.2MB fixed drive and one 360KB diskette drive.

Operating System.

- MS-DOS Version 2.0 or later.

User Interface/Ease of Use.

- Interactive questionnaires.

Documentation and Training.

- User manual.
- On-site training.
- Demonstration diskette.

Developer/Vendor. Department of Energy Center for Computer Security, Los Alamos National Laboratory, Los Alamos, NM; (505) 667-7777.

Remarks.

The LAVA methodology stresses a team approach for conducting the risk assessment. It is recommended the team be composed of people with a broad spectrum of backgrounds and expertise to ensure a thorough assessment. It is further recommended that a consensus among the group be reached before entering an answer to any of the questions, and that in some cases this may be the most difficult part of administering this risk management software.

Distribution of this package is handled through the National Security Agency (contacts include Sam Samuelson (301) 688-6022; Ed Markel (301) 688-6022; or John Lapille (301) 688-5331.

MicroSecure Self Assessment

Methodology. Qualitative. An automated software tool that will allow PC users to conduct a security self-assessment. The software analyzes the PC environment, determines the vulnerabilities, and recommends security controls. Those safeguards recommended are designed to increase security and reduce exposures in six areas to include system integrity, data security, credibility, data integrity, backup and disaster recovery, and confidentiality and privacy. The software may be customized to meet site-specific requirements.

Hardware Requirements.

- IBM PC or compatible.
- 256K memory.
- Two diskette drives.
- Graphics capability.

Operating System.

- MS-DOS 2.0 or later.

User Interface/Ease of Use.

- Menu-driven.

Documentation and Training.

- User manual.
- Computer based training course.

Developer/Vendor. Boden Associates, East Williston, NY; (516) 294-2648.

Remarks. An optional question quiz is provided at the end of each chapter of the training course.

PRISM Risk Analysis and Simulation for the PC

Methodology. Qualitative. Prism supports development of risk analysis modelling, simulation, sensitivity analysis, and graphical presentation of results. It also contains system functions to save, retrieve, display, and modify existing models. In addition to simple algebraic equations, Prism permits use of BASIC-like statements to model more complex applications.

Hardware Requirements.

- IBM PC or compatible.
- 512K fixed drive.

Operating System.

- MS-DOS 2.0 or later.

User Interface/Ease of Use.

- On-line HELP facility.

Documentation and Training.

- User manual.
- Training and on-site seminars.
- Consulting services available to assist in model development.

Developer/Vendor. Palisade Corporation, Newfield, NY; (606) 564-9993.

Remarks.

QUIKRISK

Methodology: Qualitative. Quikrisk requires the user to input information about the systems and facilities on a scenario form. These forms pertain to potential threats, current safeguards, and assets. Once all of the input information has been entered, the software computes the results which provide an annual loss exposure. An additional computation is performed which displays a return on investment for each control in place. The analyst also has the capability of modifying the results of previous computations by modifying the input data. In addition, the software is delivered with a threat file containing numerous threats and frequencies. The user has the capability of adding threats to this list.

Hardware requirements.

- IBM PC or compatible.
- Two diskette drives.

Operating System.

- MS-DOS Version 2.0 or later.

User Interface/Ease of Use.

- Menu-driven.

Documentation and Training.

- User manual.

Developer/Vendor: Basic Data Systems, Rockville, MD; (301) 269-2691.

Remarks.

RANK-IT

Methodology. RANK-IT automates the Delphi method by adding comparison risk ranking to obtain an ordinally ranked list of items. Each ranked item has a numerical value. This software is used to risk rank system threats, controls, vulnerabilities, or other alternatives. It also can be used to rank any other type of quantifiable business decision.

Hardware Requirements.

- IBM PC or compatible or IBM Personal System/2.
- 512KB memory.
- Single diskette drive or 1MB hard disk.
- Graphics capability.

Operating System.

- MS-DOS Version 2.0 or later.

User Interface/Ease of Use.

- Menu-driven.

Documentation and Training.

- User manual.
- Tutorial and training diskettes.

Developer/Vendor. Jerry Fitzgerald & Associates, Redwood City, CA; (415) 591-5676.

Remarks.

Risk Analysis System (RA/SYS)

Methodology. Quantitative. RA/SYS is an automated risk analysis system which processes with a series of interconnected files that can assess up to 50 vulnerabilities and assets and 65 threats. Calculations are performed on threat/vulnerability pairs to produce threat ratings and threat frequencies. A report summarizes loss estimates, cost benefit analysis, and return on investment.

Hardware Requirements.

- IBM PC or compatible.
- 128KB of memory.
- Two 360KB diskette drives or 640KB fixed drive.

Operating System.

- MS-DOS Version 2.0 or later.

User Interface/Ease of Use.

- Menu-driven.
- On-line HELP facility.

Documentation and Training.

- User manual.
- Technical assistance available upon request.

Developer/Vendor. Nander Brown & Co., Reston, VA; (202) 653-6646.

Remarks.

Government agencies may obtain copies of this software at no charge.

Methodology. Quantitative. An annual loss expectancy (ALE) is computed based on an answered questionnaire. Reports from this system may be displayed on the screen which summarizes the effect of a threat on different parts of the system. The user has the option of changing the values of the variables to determine various cost-effective safeguards.

The RiskCalc software is part of a 'family' of software tools listed below:

o The "Demonstration Model" allows the user to establish a site-specific questionnaire or select one that models several risk scenarios.

o Risk Minimizer identifies an organization's most significant elements of risk once the analysis is complete. The results are presented in a variety of formats. Risk Minimizer may be used with any other risk management methodology that uses the RiskCalc file format.

o The "System Administrator" provides a capability for the user to design or customize an existing risk analysis model. The user must have modelling experience and a good working knowledge of computer systems.

Hardware requirements.

- IBM PC or compatible.
- 512KB memory.
- Fixed drive is optional but recommended.

Operating system.

MS-DOS Version 2.1 or later.

User Interface/Ease of Use.

- Knowledge of microcomputer systems is required.

Documentation and Training.

- User manual.
- One day on-site training.

Developer/Vendor. Dr. Lance J. Hoffman, George Washington University, Washington, DC; (202) 994-4955.

Remarks.

RISKMAN

Methodology. Quantitative. The RISKMAN program contains files where data is entered for site-specific applications or facilities. A questionnaire allows the analyst to collect information about the organization's security environment. Responses to this questionnaire are used to calculate an annualized loss expectancy using relational databases that contain information about threats, assets, vulnerabilities, loss categories, and safeguards. A 'what-if' capability allows the user to determine the most effective security safeguards.

Hardware requirements.

- IBM-XT/AT or compatible.
- 512K memory.
- 10MB fixed drive.

Operating system.

MS DOS Version 2.1 or higher.

User Interface/Ease of Use.

- Menu-driven.

Documentation and Training.

- User manual.
- Training provided upon request.

Developer/Vendor. Expert Systems Software, Inc., Long Beach, CA; (213) 499-3346.

Remarks.

RiskPAC

Methodology. Qualitative. This software product is composed of three components--questionnaire, surveys, and reports. The results of the questionnaire are stored in a 'survey' which provides the basis of the analysis. The questions point to discrete categories that provide a review of an organization's policies, physical environment, processing hardware and the applications and data which make up a system. Each of these categories are evaluated separately. A variety of questionnaires that apply to several disciplines (e.g., manufacturing, banking, and government) are available. 'Reports' provide the results of the evaluation expressed on a scale of one to five, with five representing a worst-case scenario. The weighting and scoring algorithms are based on Kepner/Tregoe type of analysis. The package can produce data files that can be input to various database spread sheets. Further, the software is equipped with a number of utility routines that allow organizations to develop their own questionnaires. This 'System Manager' capability is available separately.

Hardware Requirements.

- IBM PC, PC/XT, or PC/AT or compatible.
- 256K of memory.
- Two diskette drives or 10MB fixed drive.

Operating system.

- MS-DOS Version 2.0 or later.

User Interface/Ease of Use.

- Menu-driven.

Documentation and Training.

- User manual.
- Training provided upon request.

Developer/Vendor: Profile Analysis Corporation, Ridgefield, CT, Subsidiary of Computer Security Limited; (203) 431-8620.

Remarks.

APPENDIX B
REFERENCES

The following list of documents, publications, and organizations provide a wide variety of information on varying aspects of risk management. The list is not intended to be all-inclusive, rather it is meant to serve as a starting point for those interested in learning more about risk management and risk analysis.

BROW88 Browne, P., Laverty, J.E., Using Decision Analysis to Estimate Computer Security Risk, Computer Security Risk Management Model Builder's Workshop, Denver, CO, May 1988.

CALS88 CALS Implementation Guide, Draft MIL-HDBK-CALS, January 1988.

COMP87 Computer Security Act of 1987, Public Law 100-235, January 1988.

DOD5200-28 Department of Defense Trusted Computer System Evaluation Criteria, December 1985.

FIPS65 Guidelines for Automatic Data Processing Risk Analysis, National Bureau of Standards, August 1969.

FIPS31 Guidelines for Automatic Data Processing Physical Security and Risk Management, National Bureau of Standards, June 1974.

GUAR88 Guarro, S., Analytical and Decision Models of the Livermore Risk Analysis Methodology (LRAM), Model Builder's Workshop, Denver, CO, May 1988

HOFF86 Hoffman, L., Risk Analysis and Computer Security: Bridging the Cultural Gaps, Proceedings, 9th National Computer Security Conference, sponsored by the National Bureau of Standards and National Computer Security Center, September 15-18, 1988.

HOFF88 Hoffman, L., A Prototype Implementation of a General, Risk Model, Computer Security Risk Management Model Builder's Workshop, Denver, CO, May 1988.

JACO88 Jacobson, R., IST/RAMP and CRITI-CALC: Risk Management Tools, Computer Security Risk Management Model Builder's Workshop, Denver, CO, May 1988.

KATZ88 Katzke, S., A Government Perspective on Risk Management of Automated Information Systems, Computer Security Risk Management Model Builder's Workshop, Denver, CO, May 1988.

MAYE88 Mayerfeld, H., Definition and Identification of Assets as the Basis for Risk Management, Computer Security Risk Management Model Builder's Workshop, Denver, CO, May 1988.

MOSE88 Moseleh, A., A Matrix/Bayesian Approach to Risk Management of Information Systems, Computer Security Risk Management Model Builder's Workshop, Denver, CO, May 1988.

OMB130 OMB Circular No. A-130, Management of Federal Information Resources, December 1985.

SMIT88 Smith, S., LAVA: An Expert System Framework for Risk Analysis, Computer Security Risk Management Model Builder's Workshop, Denver, CO, May 1988.

SNOW88 Snow, D., A General Model for the Management of ADP Systems, Computer Security Risk Management Model Builder's Workshop, Denver, CO, May 1988.

SOCIETY Society for Risk Analysis, 8000 Westpark Drive, Suite 400, McLean, VA 22102.

SP500-109 Overview of Computer Security Certification and Accreditation, National Bureau of Standards, April 1984.

SP500-133 Technology Assessment: Methods for Measuring the Level of Computer Security, National Bureau of Standards

SP500-153 Guide to Auditing for Controls and Security: A System Development Life Cycle Approach, National Bureau of Standards, April 1988.

WHIT88 White, G., Mate, K.V., Air Force Experience with PC Based Risk Analysis Systems, Computer Security Risk Management Model Builder's Workshop, May 1988.

SECURITY

Computer Security Issues in the Application of New and Emerging Information Technologies

CALS SOW TASK 5.3

COMPUTER SECURITY ISSUES IN THE APPLICATION OF NEW AND EMERGING INFORMATION TECHNOLOGIES

Prepared for the

COMPUTER-AIDED ACQUISITION AND
LOGISTIC SUPPORT (CALS) PROJECT OFFICE
DEPARTMENT OF DEFENSE

MARCH 1989

Prepared by

DENNIS M. GILBERT
BRUCE K. ROSEN*

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
NATIONAL COMPUTER SYSTEMS LABORATORY
COMPUTER SECURITY DIVISION
*INFORMATION SYSTEMS ENGINEERING DIVISION

COMPUTER SECURITY ISSUES IN THE APPLICATION
OF NEW AND EMERGING INFORMATION TECHNOLOGIES

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

The authors would like to thank the following people for their assistance in the preparation of this document: William Bur, Ted Landberg, Roy Morgan, Miles Smid, Dennis Steinauer, and Robert Warnar. Their input and encouragment are highly appreciated.

EXECUTIVE SUMMARY

Introduction

The Computer-Aided Acquisition and Logistic Support (CALS) program is both a concept and strategy by which the Department of Defense (DoD) is attempting to apply modern digital computer and telecommunications information technology for use in DoD and its industrial support structure during the life cycle of DoD weapon systems.

DoD and its CALS program face an environment shared by other federal agencies and other organizations. Some important elements of this environment are:

- information systems are an increasingly integral part of business activity; there is increasing pressure to be more productive and competitive; application of new and emerging technologies is a major element in improved productivity and competitiveness

- key factors in that productivity and competitiveness are: system integration, compatibility and interoperability among system elements; use of products available from a variety of sources which incorporate marketplace-accepted standards; and the ability to securely and conveniently access information resources and data in a variety of forms in widely dispersed locations

- computer security fosters the introduction and application of new technology; appropriate computer security must be integral, not peripheral, to increased productivity and competitiveness; productivity gains, cost savings, and payoffs cannot be optimally achieved without integrating a total systems' information security in the same way that 'islands of automation' in large, complex systems need to be integrated

- there is growing sensitivity about individual and organizational privacy and confidentiality; there is growing importance in the integrity of our information resources, the confidence in which they are held, the trust placed in those who administer the systems, and the safeguards built into the systems themselves

- the application of new and emerging technologies present unique information security opportunities and challenges

The confidentiality and integrity of CALS data and the reliability and availability of its systems' components are vital to CALS successful implementation.

This report explores the role of information security and its impact for CALS on the productivity of its information systems that employ new and emerging computer application technologies. Areas covered in the report include: memory and smart cards, optical disks, artificial intelligence, and telecommunications and networking. These areas were chosen because of their potential as candidates for addressing the large variety of CALS information security and application requirements.

These subject technology areas are viewed both as tools for implementing and improving information security, and as presenting information security issues, opportunities, and challenges in their application. The report's primary area of concentration is on the application of these technologies in a personal computer or workstation environment, although much of the information presented is also applicable in an environment utilizing a large mainframe type system.

The purpose of this report is to provide CALS management and those involved with CALS implementation with an overview of the relationships among information security issues and the application of these new technologies. Only after achieving an understanding of these new technologies and their related security issues will it be possible to focus on the potential opportunities, risks, vulnerabilities, and safeguards that will likely be at issue as CALS evolves.

The remainder of this Executive Summary briefly describes each of the new technologies covered in this document. Included in the main body of this document is a look at how others (government and industry) are using each technology, a discussion of how CALS might use each technology, and an examination of how each technology either enhances required security or introduces vulnerabilities that must be addressed. Additional computer security issues, including Data and Database Administration considerations are also discussed.

Memory and Smart Cards

Four types of memory and smart card technologies are addressed: embossed plastic and magnetic stripe cards; chip or smart cards; laser memory cards; and light signatures. These cards and

technologies are candidates for use by CALS to improve computer security in: personal identification and access control to facilities and resources; authentication and access control to computer data and resources; audit trails of access to sensitive data; and prevention of forgeries.

These technologies are used in the private sector as financial transaction cards (including credit cards and automated teller machine cards), with access control and data carrier functions becoming increasingly important (especially for medical applications). Federal agencies are moving toward the use of these technologies in benefits and eligibility transaction processing and access control. CALS will be especially concerned with the confidentiality and integrity of the digital data which is at its core. It will become increasingly important for Data and Database Administrators to work with security specialists to ensure that the needed protection is in place. As information security requirements become increasingly pressing, integrated circuit-based smart cards, with their secure architectures, alone or used in conjunction with biometric devices and encryption, will be increasingly attractive. Deciding which technology to use and when to use it is a complex function. Some of the elements of this complex function are perceived risk, security features of each technology, costs to transition to new ways of doing business, and provider and user acceptance.

Optical Disks

Optical disks provide for vast amounts of data to be stored on optically sensitive media. Three optical disk technologies are: compact disk-read only memory (CD-ROM); write once read many times (WORM); and erasable. CD-ROM disks, which use basically the same technology as compact disk-audio (CD-Audio), can be read by computer equipment, but cannot be written on by computer equipment. WORM disks can be written to once by computer equipment and can be read repeatedly, but WORM disks cannot be rewritten in areas that have been previously written. Erasable disks can be written to and read from repeatedly, in a manner analogous to that of magnetic disks. In the private sector and in the federal government, CD-ROM is used primarily as a medium for publishing and distributing data, both for external sale and for in-house distribution. WORM technology is primarily used for data archiving and for audit trails. Erasable disks are used for large data storage and retrieval. CALS will likely use these technologies in comparable ways.

A significant issue associated with the use of these optical

technologies is the increased risk associated with the possible compromise of a large amount of an organization's data. CD-ROM has the advantage that, because it is prepublished, it cannot be modified and may be difficult to forge. WORM technology provides for an audit trail capability that might not otherwise be available. Erasable disks have many of the risks associated with magnetic disk. Because of their large storage capacities, WORM and erasable disks may be difficult to backup. Another security concern related to all three types of disk is how to control access to portions of the disks in multi-user multi-application environments. Because of the amount of data stored, another issue is the risk associated with an authorized or unauthorized user being able to access separate pieces of information, and through the use of aggregation and inference, obtain unauthorized information. Protection against all of these data access-related problems will be of primary concern to Data and Database Administrators.

Artificial Intelligence

The branches of artificial intelligence (AI) include: expert and knowledge-based systems; natural language interpretation and continuous speech recognition; machine vision and robotics; and knowledge and processing, cognition, pattern recognition, process control, neural networks. Progress is being made in each of these areas. However, by far the most development and practical application is in the area of expert and knowledge-based systems, where programming tools are available that allow the knowledge of an expert in a given field to be captured and then applied to problem solving directly by an automated system. This is true in both the private sector and in the federal government and it is also highly likely to be true of the CALS environment.

In recent years, AI in general and expert systems in particular, have come out of the laboratory and the universities and have become a serious tool of business and industry. They are currently being employed in the areas of: quality control in manufacturing; maintenance and diagnostics; inventory control; resource scheduling; claims processing and insurance adjusting; optimizing and customizing systems; fleet monitoring and readiness planning; vessel stress analysis; risk management; and training. It is likely that CALS will increasingly apply AI technology to a variety of data intensive activities and problems including engineering design, test and evaluation, maintenance, training, and contract management.

CALS also will likely use AI to enhance its information security by using it for risk assessments; access control,

identification, and authentication determinations; and intrusion detection where AI or non-AI tools may be applied by a non-authorized user. AI techniques may be useful in multilevel environments, where some users are not cleared for the most sensitive data on the system and where the implementation of formal access control models to determine the likelihood of possible inference violations or to determine if they have occurred is extremely complex. The use of AI for diagnostics and feedback during product design can increase system reliability. Use of AI techniques by Data and Database Administrators to design in needed database security functions will become increasingly important.

In using AI technologies, CALS needs to be concerned about the concentration and protection of sensitive information and resources including the inference rules that are embodied in an application. These rules could form databases requiring extreme levels of protection. CALS will also have to become increasingly concerned about the integrity of very large and complex AI systems which may not have been fully tested.

Telecommunications and Networking

Telecommunications will be integral to CALS operations. Among the purposes for establishing a telecommunications network are: resource sharing; data sharing; direct or on-line communications; and access to electronic mail or bulletin board facilities.

The first type of network that is of concern to CALS is that in which a limited number of people are connected to each other and shared resources over a limited geographic area (e.g., a building or a campus) on a local area network (LAN). However, in a short time even LAN users will seek to use services that are remotely located including electronic mail, bulletin boards, or on-line information, financial, or other services. Thus CALS can not, at the outset, just be concerned with LAN problems, but must be concerned with the myriad of problems of all types of telecommunications facilities.

Concerns of telecommunications users are: the availability of the connection or link; the ease of sending and receiving data and using network resources; the integrity and confidentiality of transmissions; the ability to identify themselves to the system; and the ability to know that the other party to a transmission is authorized to take the action that they are taking.

The types of information communications that might be required in the CALS environment include: data, graphics, and text;

information about information (formats, etc); administrative and operational communications; bulletins, emergency action notices; routine electronic mail; procurement-related announcements, documents, inquiries, responses; access paths to remote information sources; design-related communications; test procedures, instructions, data, results; and CALS committee communications including announcements, agendas, minutes, and ballots.

The basic considerations for network telecommunications security also apply in the CALS environment, but are intensified. This is caused in part by: the sensitive nature of CALS data such as weapons systems and deployment information, procurement sensitive information, and company proprietary information; the great geographic dispersion of CALS data and users; and the sheer magnitude and complexity of CALS which makes management and control a particularly challenging problem.

Among the major telecommunications security concerns of CALS is the management and operation of individual CALS networks and the whole communications environment. Of issue is the degree to which information security responsibilities will be centralized. Related concerns are the determination of which channels are secure or insecure, and the requirements for access mediation and discretionary and mandatory access controls. Also, there exist the problems of who certifies that the appropriate network controls are in place and how this certification is accomplished.

Encryption will definitely be necessary for some CALS-related communications. CALS faces the critical communications security questions of which cryptographic tools and technologies will be used and how related keys are to be managed.

Other information security issues for CALS relate to the prevention and detection of, and the recovery from, the effects of viruses and other such security related software problems. Also at issue is the availability of alternative paths or backup and recovery procedures in case of line failures or other network or system interruptions.

New Technologies, Standards, and Computer Security

CALS has recognized the need for standards and specifications, and in its incremental approach, CALS adopted existing or emerging national standards and specifications which fall into the following basic categories: functional requirements standards; data interchange standards; data management and access standards; communications protocols; and application guidance. Thus far, aside from communications, either standards and

specifications particular to the technologies being examined have not been developed, or they have not been embraced by CALS. Neither have information security related standards been adopted for use by CALS. However, in the Data and Database Administration area, use of the recently approved Information Resource Dictionary System (IRDS) standard could provide Administrators with the first of many needed tools to tackle the data security problems inherent with these new technologies.

Conclusion

Computer security is vital to the successful implementation of CALS. The new and emerging technologies discussed in this report are prime candidates for application in accomplishing CALS goals. They may be necessary in achieving the required levels of information security, or they represent potential vulnerabilities that must be addressed. Knowledge about both information security and the new and emerging technologies is necessary for those engaged in CALS-related activities. Therefore, it is recommended that the CALS Project Office:

- conduct an overall risk analysis and develop a global information security architecture and models, along with appropriate regulations, by which those who have information security responsibility may be guided

- initiate a study to select a set of short term, specific objective pilot projects, that could be utilized to explore these technologies and their security implications

- establish the needed procedures, and fund the necessary work, to ensure that information on technologies, tools, techniques, policies, procedures, and baseline standards and specifications be widely disseminated to the CALS community in a friendly, practical format, such as an information computer security CD-ROM which incorporates needed information for CALS program managers, Data and Database Administrators, and contractors.

As the move in CALS, and elsewhere, is toward a more digitized world, the legal status of digitized records that replace hard copy is uncertain. Various forms of digital signatures to authenticate individuals, workstations, tokens, transactions, and processes will be required. This will pose both legal and technical challenges to CALS. Accordingly, the CALS Project Office should, on a regular basis, examine the legal and

regulatory status of digitized records to ensure that no activities are occurring under CALS that are in conflict with the appropriate legal precedents, or regulations.

Finally, in this report, information security has been addressed in the context of a number of new and emerging technologies. It is important to note that the fundamental principle on which all security rests is that of individual responsibility and accountability. Thus it is critical to develop an environment of trust and awareness that encourages the individual to be conscious about, and a willing participant in, protecting that information and those resources with which he or she is entrusted. This is especially true since, as this document shows, some of these new technologies increase dramatically the dangers of compromise or loss of large volumes of information. However, as this document also demonstrates, when utilized properly by the various areas of an organization concerned with systems and information security, these new technologies can serve as excellent tools in the fight against loss or compromise of an organization's information resources.

COMPUTER SECURITY ISSUES IN THE APPLICATION OF NEW AND EMERGING INFORMATION TECHNOLOGIES

I. INTRODUCTION AND OVERVIEW

A. Background and Reason for the Document

The Computer-Aided Acquisition and Logistic Support (CALS) program is both a concept and a strategy by which the Department of Defense (DoD) is attempting to apply modern digital computer and telecommunications information technology for use by itself and its industrial support structure in the life cycle of Defense weapon systems.

1. The Environment

DoD and its CALS program face an environment shared by other federal agencies and other organizations. Some important elements of this environment are:

- information systems are an increasingly integral part of business activity; there is increasing pressure to be more productive and competitive; application of new and emerging technologies is a major element in improved productivity and competitiveness
- there is a need to increase productivity and improve competitiveness, some of the keys to which are: system integration, compatibility and interoperability among system elements; use of products available from a variety of sources which incorporate marketplace-accepted standards; and the ability to securely and conveniently access information resources and data in a variety of forms in widely dispersed locations
- computer security fosters the introduction and application of new technology; appropriate computer security must be integral, not peripheral, to increased productivity and competitiveness; productivity gains, cost savings, and payoffs cannot be optimally achieved without integrating a total systems' information security in the same way that "islands of automation" in large, complex systems need to be integrated

- there is growing sensitivity about individual and organizational privacy and confidentiality; there is growing importance in the integrity of our information resources, the confidence in which they are held, the trust placed in those who administer the systems, and the safeguards built into the systems themselves

- the application of new and emerging technologies present unique information security opportunities and challenges

2. Report Overview

a. Rationale for selection of technologies

This report explores the role of computer security and its impact on the productivity of CALS information systems that employ a variety of new and emerging computer technologies. Areas to be examined will include memory and smart cards, optical disks, artificial intelligence, and telecommunications and networking. These technologies were chosen for examination because of their potential for application in the CALS environment.

The CALS implementation strategy [OASD88] addresses the modernization of the technical information system infrastructure for weapon systems. This includes engineering data repositories, technical manual production systems, supply and distribution information systems, and procurement contract data management systems. The modernization "will anticipate and be compatible with the relevant CALS electronic information interchange standards and take full advantage of the more-nearly-paperless world that the CALS program will establish." The technologies that are explored in this report are likely to be integral parts of that infrastructure. The technologies will also be integral to the CALS management infrastructure.

b. Approach

Each technology is briefly described, followed by a look at how others (government and industry) are using the technology. Potential ways in which CALS may use each technology is then presented. Next is a discussion of how the technology either enhances required information security or introduces vulnerabilities that must be addressed. Also, additional information security issues are presented.

Finally existing and emerging standards (defacto and other)

related to computer security in the CALS and other environments are identified. The report is then summarized, and recommendations are presented.

c. Perspectives

The technologies presented in this report are examined individually. However, an underlying theme is that the application requirements facing the CALS community and the application of these technologies can and should be viewed in an integrated way so as to support CALS objectives and provide and enhance needed computer security.

No attempt is made to examine all of CALS functional or computer requirements or all CALS computer security requirements. However, this publication does address those functions and requirements which could be satisfied by the technologies being discussed and those computer security requirements that can be enhanced by the use of those technologies.

Reference has been made to CALS documentation and discussions that have been held with persons familiar with the CALS environment. This is complemented by professional judgments in forecasting what technologies may be used by CALS and how they may be used. Regardless of the particular decisions eventually made, the information security issues discussed here should be applicable to a variety of CALS implementation strategies and technologies.

The theme of database permeates the whole of CALS. These databases will be in many forms and formats and occupy a variety of media. They may be located within a single system or distributed among many widely separated systems. They may exist as fields of tabular, text, graphics, video, or audio data. The success of the CALS will depend on: how well the data is managed, how well it is converted to useful information, and how well its availability, integrity, and confidentiality are provided for throughout its life cycles. This report can contribute to that success by helping those considering the use of these new and emerging technologies make more informed judgments about the information security potentials and tradeoffs associated with their use.

B. CALS and Information Security

1. Information Security Concerns

DoD, through CALS, is evolving toward a target system that employs such elements as intelligent gateways, wide area networks, and distributed databases for the distribution of logistics products. The integrity of CALS data and the reliability and availability of its systems' components are vital to CALS successful implementation and operation, as are related concerns about confidentiality, disclosure, and access control. According to [OASD87], the following are among the CALS data security concerns:

- security and control of automated data (a common concern to all areas of information resource management)
- management of classified and proprietary data, release approval, and user access to in-process information
- safeguarding of aggregated data
- integrated databases and on-line user access
- incorporating solutions to data management problems in its technology development planning

The DoD CALS Communications Working Group and the CALS Industry Security Task Group are working to define policy and technical issues and potential solutions among those being developed by the National Security Agency (NSA), the Defense Communications Agency (DCA), the National Institute of Standards and Technology (NIST), and industry.

2. Data Protection

The CALS Implementation Guide [DOD88] discusses security and related issues and refers to new methods and techniques for protecting against unauthorized use and dissemination. The government and defense contractors have spent large sums of money to protect their data. The technical and logistics data that will be maintained on government and contractor hosts will have a variety of sensitivities. They may be company proprietary, competition-sensitive, or classified. When information is integrated, a mosaic effect may occur. A mosaic effect results when non-sensitive material in aggregation can produce sensitive

information. This effect can also occur when information of low levels of classification, or sensitivity, are integrated, thereby creating information of a higher level of classification or sensitivity. Thus, a mosaic effect can occur with information that is:

- o unclassified to For Official Use Only
- o industry or corporate proprietary
- o classified (confidential, secret, top-secret)

Security specialists alone will never be able to determine what combinations of data could result in a mosaic effect. Research projects must be conducted concerning this problem, while at the same time, it must become the responsibility of the Data and Database Administrators to work with functional area specialists to determine which possible combinations of data must be protected. Data Administrators must make clear to these functional area specialists that they must be concerned not only with data in their own area being combined, but they must also help in the consideration of data between different functional areas being combined. Then, working with security specialists and researchers, the Data and Database Administrators must determine how to best protect against the mosaic effect. Finally, the Data and Database Administrators, along with the security specialists, must implement the needed protections.

[DOD88] refers to the "Orange Book" [DOD85-1] which provides criteria for determining the protection level of information processing products. One level described is "system high" where all users of a system must have clearance at least as high as the highest security level of any data on the system. Another level is that of "multilevel security" where some users of the system have a lower clearance than required for some of the system's data. The system must therefore be able to protect higher classified data from those who have legitimate access to only lower classified data. [DOD88] also refers to National Security Decision Directive (NSDD) 145 "National Policy on Telecommunications and Automated Information Systems Security," as defining interrelationships and interdependencies between telecommunications and computer systems.

3. Other Threats and Vulnerabilities

The Implementation Guide focuses on unauthorized use and

dissemination. While this is certainly important, it does not represent the full extent of computer security threats and vulnerabilities and challenges to the systems under CALS. Errors, omissions, and environmental incidents are among the items that can also impact the confidentiality, integrity, and availability of the data and resources needed for the successful operation of CALS.

In CALS, there is an additional dimension to the mosaic effect problem. Through CALS, data may be gathered and aggregated not from just one source, but from many sources including both government and industry. This data could be combined with other information in the public domain or readily available to produce sensitive or unauthorized information. Examples of public domain data are those from financial and other information sources like Dunn and Bradstreet, census information, patent and industry information, Congressional Record, Commerce Business Daily, or reports of industry watchers.

4. Adequacy of Current Information Security Technology

Security concerns in CALS Phase I relate to the protection of data in the transition from hard copy to digitized form. Concerns in Phase II relate to user validation, data aggregation, and database integrity. It is generally felt by those committees and groups addressing CALS that existing technology is adequate for Phase I, but that new techniques and technologies will have to be implemented for Phase II.

[OASD88], in addressing advanced product information technology projects, indicates that data security is significant in addressing issues concerning technical data exchange. It notes that such technical data requires various levels of security protection and, when technical data is aggregated in databases, sensitivity and security issues are raised. These and other computer security issues are being addressed by the NSIA CALS Industry Security Task Group, whose guidance will be released in 1989. The report indicates that security for CALS Phase I data interchange should be adequate; Phase II requirements are being explored by government and industry and that new data security technology will be included in Phase II implementation, beginning in 1991.

5. CALS Security Documentation

Documents that must be used by government and contractors in addressing CALS information security include:

- Industrial Security Manual, DOD 5220.22-M - which is used to establish security requirements for a given maximum data sensitivity and minimum clearance, or authorization of a system user to a computer security category, ranging from C1 to A1

- Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments, CSC-STD-004-85 - which is used for information on product evaluation

- DD Form 254, DoD Contract Security Classification Specifications - which is used by DoD weapon system and data system acquisition managers and security managers to communicate requirements to industrial support

Information on acquisition policy related to data rights, privacy, and legal liability will be produced by the CALS Acquisition Working Group. (See FY 89 update to the CALS Implementation Guide).

C. Information Security Background

1. Basics

An organization has things worth protecting - data or information, people, software, hardware, facilities (including utilities), communications, media, etc. These things are often referred to as assets. These assets are exposed to a variety of impending dangers or threats, which can take advantage of susceptibilities or vulnerabilities. Through a variety of safeguards (technical, administrative, physical, and personal) the goal is to prevent, or at least minimize (reduce the frequency or probability), the destruction, modification, or disclosure of information or resources that are sensitive to the organization, or that the organization is entrusted with protecting. Failing that, the goal is to ensure the detection of such adverse activities, and provide for total recovery of any lost, modified, or otherwise damaged information or resources. Adverse activities or threats could occur due to accidental, malicious, or natural acts or design limits. There are clearly

costs associated with the replacement of assets or the loss of the confidentiality, availability, or integrity associated with them.

Security is necessary to prevent undesirable events where possible, to deter them if prevention is not fully practical, to minimize the impact of the events if they occur, and be able to detect if something has happened and to recover as best possible.

In dealing with new and emerging technologies as in dealing with traditional data processing there is still a need to protect assets in a way that minimizes the costs, commensurate with the risks involved.

2. Definitions

Throughout the discussion, each new and emerging technology needs to be evaluated on the degree to which it enhances or threatens the confidentiality, integrity, and availability of the information systems to which they are applied. The following definitions are applicable [LONG87].

By **confidentiality** we mean:
- that individual access to data is based on authorization by the information owner or custodian
- there exists adequate protection against compromise and inadvertent disclosure

By **integrity** we mean:
- that under all conditions the system reflects the reliability and correctness of the operating system and all protection mechanisms
- there exists adequate protection against undetected alteration of data
- that data and data structures are accurate and consistent

[COUR88] offers that integrity means that an a priori assumption of quality in the context of intended usage or application has been met.

By **data integrity** we mean that data reflects its source document and that it has not been exposed to accidental or malicious alteration or destruction. By **system integrity** we mean that an ADP system is based on a correct and reliable operating system and that it includes all needed protection mechanisms.

Availability refers to the notion that computer resources will be

available to authorized users when needed.

By **authentication** we mean:

- there exists adequate protection against fraudulent transmission by establishing the validity of a transmission, message, station, or originator
- that everything about a teleprocessing transmission and the message has not been altered or corrupted or stored and retransmitted by a third party
- the identities of individuals are verified by an established process

3. Encryption

Encryption refers to converting or transforming data from an intelligible or plain text form to an unintelligible or cipher text form by means of an algorithm and the use of a key. The reverse process, **decryption**, refers to transforming cipher text back to plain text, also with the use of a key that may be the same or different from the one producing the encrypted data. Regardless of which technology is being addressed in this report, it may be necessary to protect data from those not authorized to have access. Encrypting data during one, many, or all of the phases of its life cycle may be the only viable way to achieve this protection. The Data Encryption Standard (DES) algorithm, specified in the Federal Information Processing Standard-46 (FIPS 46), is required in Federal government applications for the cryptographic protection of computer data (unless the data is classified according to the National Security Act of 1947 or the Atomic Energy Act of 1954 and their amendments). Non-federal organizations may, and do, use DES. For more information see [FIPS88] [FIPS85-1] [FIPS85-2].

4. Managing Risk

It is not possible to have a risk-free environment. The objective is to manage and minimize the risk. The technologies being examined in this report can help in that process. They do not, however, change the fact that the greatest threat to an information system is typically not from the outsider trying to break in, but rather, it is from the insider who is authorized access to the system, but who misuses that position. For this reason, despite the availability of assists from technology, it is still necessary for each organization to have an information policy that incorporates the awareness and training of its employees and embraces the concept of individual responsibility

and accountability for the information and systems being used. This must be combined with the implementation of appropriate levels of controls. Additionally, the organization must protect itself against not only the willful acts, but also against "pools of the incompetent and untrained" who are subject to errors of both omission and commission. While the technologies discussed in the following sections can be applied to help an organization protect itself, they can also increase the danger to the organization since they can also multiply the capabilities of the "bad" user to corrupt, destroy, or misuse the organizations data processing assets.

II. MEMORY AND SMART CARDS

A. Description of the Technologies

1. Overview

This section discusses a variety of technologies that employ either a plastic card (similar to the common credit card or Automated Teller Machine (ATM) card) or a differently shaped plastic container or token, that can be carried and used by an individual. They provide combinations of capabilities including those to store information, allow reading from and writing to information storage locations, control access to portions of that information, and to perform logical and computational operations. Each particular combination of technologies used will produce a unique set of costs, functional capabilities, vulnerabilities, and security capabilities. These technologies can be used in a wide variety of applications. However, they are examined here primarily from the perspective of being tools for enhancing security in terms of confidentiality, integrity, and availability of the data and systems of concern. While a card or token may be used exclusively as a data carrier, more often, the data on the card or token is used to support such functions as:

- personal identification
- controlling access to computer and data resources
- controlling access to facilities and other resources (e.g., supplies, materials)
- authentication of data, transactions, and processes

Personal identification is integral to all other access control and authentication activities. Three means to identify a person involve presenting singly or in combination:

- something he or she has
- something he or she knows
- something he or she is

Each type of card or token provides different combinations of features to support security objectives. The types of cards and tokens to be discussed in this document are:

- embossed plastic and magnetic stripe
- smart card (sometimes called chip or integrated circuit (IC) cards)
- laser memory
- light signature

(Note: Material in this discussion is drawn heavily from [SVIG85].)

2. Embossed Plastic and Magnetic Stripe Cards

Embossed plastic cards have raised letters or numbers that are created from pressure on various portions of a plastic base. In some cases the cards are presented and visually inspected. In other cases they are used to imprint on paper the embossed information which typically contains account and issuer identification and data (e.g., expiration date). They are frequently used to purchase gas for automobiles and for other retail products and services. They are also in common use as a means of identifying the bearer as being entitled to certain services. For example, embossed cards may be used at a hospital to imprint identifying and account information on a patient's treatment or prescription forms. Embossed cards may also be used to permit withdrawals from an organization's warehouse or storeroom, or they may be used to allow access to an organization's facilities such as a school cafeteria, library, laboratory, sports center, or parking lot.

In the 1950's the airline, banking, travel, and entertainment industries began making extensive use of handheld plastic cards for financial transactions. Magnetic stripes were an attempt to provide an automatic means of entering the 19-digit identification codes of the embossed plastic cards in order to address entry-error rates in an economic manner. Additionally, they expanded the amount of information that can be stored on the card and enhanced the security of the card. This made the card less subject to unaided reading of its data and less subject to forgery.

By the 1970's there had been world-wide acceptance of these cards in financial transactions (including ATM machines) with total issue reaching one billion in the 1980's. [SVIG85 pp20-22]. Many of these cards are reissued on a one to two year basis. This indicates wide acceptance, usage, experience, and

marketplace success, suggesting broad familiarity. Although the magnetic stripe duplicates the embossed information, most magnetic stripe cards also have embossing to permit a transition over time from an installed based of terminals that cannot read the magnetic stripe to those that can read the stripe.

While a chief purpose of the magnetic stripe data was to provide a rapid and accurate entry of the customer's identifying number, [SVIG85 p28] notes that as more data is included on the card for decision making, it then becomes a more tempting target for fraud. This is also true of the other technologies that are being examined.

[SVIG85] refers to the term financial transaction card or FTC when these cards are used in applications that have a financial base. Currently, such transactions are by far the most active use of these technologies. American standards for FTCs have been developed by the American National Standards Institute's (ANSI) accredited Technical Subcommittee X3B10 and are essentially the same as the international standards generated by the International Organization for Standardization (ISO). Among the items covered by these standards are the size, format, and content of a stripe of magnetic material that is attached to the plastic base. Other standards cover such things as dimensions, layout, materials, special features such as signature panels of the physical card; location, content, and optical recognition codes of embossing; materials, location, recording; and the structure, assigned codes, registration process, and registration authority for the account numbering.

It is claimed by some that the magnetic stripe provides only minimal protection of its information content, and can be viewed, modified, or forged with a minor investment in components readily available from retail electronic component stores. Additionally, the data capacity of the magnetic stripe can be limiting.

The cards may or may not have a photo ID. They may or may not have a signature section. Many vendors require an additional item of identification, such as a drivers licence that has both a photo and a signature of the licensee. In current practice, this extra information from the drivers license is then transferred by hand on to the appropriate document such as a check to be cashed. Vendors have been slow to automate this process by making that information machine-readable (e.g., barcodes, other optical scanning, smart card, etc.)

It should be noted that although most of the cards and tokens have a plastic base, they can be made of other materials; military dog tags for instance, may have embossing or reverse

embossing on a piece of metal. It should also be noted that there are cards currently in use that only have embossed information and do not have any form of magnetic stripe attached. These cards address only the first of the elements of personal identification, something the person has. They are less secure than a card which also provides some additional means of identification. Embossed plastic is inexpensive to produce (a few cents per card), but it provides very little storage capacity and it operates in a read-only mode.

3. Chip or Smart Cards

In a financial environment, a vendor wants to be assured that the person presenting himself or herself is who he or she claims to be, is authorized to perform the requested activity, has not exceeded designated thresholds, and, if applicable, is capable of paying for what is requested.

Despite their proliferation and the huge base of installed terminals and workstations that supports their use, magnetic stripe cards and embossed plastic cards have limitations. The amount of data storage and the degree of protection that they offer are increasingly restricted relative to the uses to which they are being put. Thus, related fraud and abuse have grown as the transaction and dollar volumes of their use have grown.

To address some of these limitations, a type of plastic card, frequently referred to as "smart card" has been introduced. Although smart cards share many things in common with cards such as embossed plastic and magnetic stripe cards, the distinguishing characteristic of them is that they have a microchip embedded in the plastic, usually in the upper left quadrant of the front of the card. This chip provides, as a minimum, a data storage capability greater than that available on a magnetic stripe card. Additionally, they usually provide processing and logic capability.

It should be noted that there is some controversy over what is or is not a smart card. [HAYK88] provides the following definition:

> "A smart card is a credit-card-sized device containing one or more integrated circuit chips, which perform the functions of microprocessor, memory, and an input/output interface."

It uses the term "smart token" for devices which otherwise satisfy the definition, but which are not standard credit card

size.

Most smart cards and tokens consist of microprocessor and various type of memory including: read only memory (ROM) usually 1K (K = 1,024) to 16K, or RAM of 128 to 256 bytes. The latter may be either Electronically Programmable Read-Only Memory (EPROM) or Electronically Erasable Programmable Read-Only Memory (EEPROM). There will be one or more integrated circuit chips for these functions. The architecture of the chips is such that there are "secret" portions of the chips which cannot be accessed externally and which contain such items as an operating system, initial and permanent keys and passwords, and encryption algorithms. This architecture creates a highly secure environment which can store sensitive information, including biometric data about the bearer, and which cannot be penetrated by an unauthorized person. Any such attempt renders the card inoperable without yielding the sensitive data.

4. Optical Memory Card

Another type of card technology is that of the laser memory card. This is a handheld, credit card-size device that has a stripe of optical sensitive material that can hold large amounts of information (ie., one to four million megabytes, depending on the size of the optical stripe). The card is read and/or written with a laser beam, and a reader/writer with such a mechanism is required. Such cards are designed for use in health and medical applications, publishing systems, record keeping systems, and transaction systems. Although there are a number of large applications of this technology abroad, especially in Japan, the large scale application of these cards has been slow in the U.S.

5. Light Signature

This technology addresses the authenticity or identification of the media rather than the authenticity or identification of the person. By means of a process which they call "signaturization", its developer, Light Signatures Inc., is able to take advantage of the inherent randomness of physical media and obtain a unique signature or fingerprint from plastic cards, paper media, and other products in order to, among other things, prevent counterfeiting.

The protection against forging the media may be sufficient on its own, or it may complement other security techniques. These techniques are now being applied for use with stock certificates and other financial instruments. Ironically, some card and media

manufacturing techniques produce such uniform composition, that small quantities of impurities must sometimes be added to establish a unique 'fingerprint.'

6. Reading, Writing, and Terminals

Most of the cards discussed to this point require use of some type of physical reader device. Of these, most use the type of reader where the card makes contact with the reader. There are also systems that do require a reader, but the readers are "contactless." That is, they do not make physical contact with the card, but instead read it by means of inductive coupling. Other cards that do not require a reader at all are referred to as "readerless." Typically, these are used in "challenge and response" environments, where a "challenge" from a host is entered into the card's keypad producing a "response" that is entered into the terminal's keyboard and transmitted to the host as part of an identification and authentication process.

In general, embossed plastic cards and magnetic stripe cards are used in a read only mode. Smart cards, as indicated, contain various sections, some of which are read only, some of which are write once, and some of which can be written over (erasable). Additionally, some portions, containing secret codes and control software, are hidden and designed so that unauthorized access attempts are destructive to the chip's operation. Laser memory cards can both be read and written to. Light signature, once initialization has occurred, is a read only process.

Both magnetic stripe cards and chip cards will typically be used with an ATM terminal, a point-of-sale terminal, or an access control key lock.

B. Current and Potential Applications for CALS and Others

1. General

The emphasis for the remainder of this memory and smart card section is on chip or smart cards since they are the most interesting in terms of CALS and computer security. However, the other technologies are not excluded and it is important to be aware of the security strengths and vulnerabilities of these technologies, too. Some of the discussion of smart cards is from the perspective of the banking industry and their use as FTC's. The discussion is still applicable to the CALS environment because many of the interactions among the CALS components and the vendor community will involve the use of the

same tools which business and industry are currently using.

The variety of cards that we have been discussing have been put to a wide range of uses and many others are being planned. These uses generally fall into the following categories, some of which have been previously mentioned:

- o control of access to facilities and other resources
- o control of access to computer resources and data
- o financial transaction card
- o identification of individuals
- o authentication and authorization
- o tracking (transactions, parts, correspondence, etc.)
- o data carrier, data storage, data publishing

This potential, plus the utility and convenience of the cards, suggests a proliferation of applications. Other countries have been and are actively exploring the use of these technologies. For example, France and Japan, which pioneered in their use, are employing smart cards as credit and debit cards in major real world banking and telephone call payment applications.

2. Federal Government Activities with Card and Token Technologies

a. Categories of applications

The U. S. has only recently begun to undertake serious projects involving smart cards. The federal government and also many state and local governments have begun to use cards and tokens and have plans for many new applications. These include:

- o receipt and processing of filing statements
- o access to government program information
- o benefit eligibility determination
- o payment of benefits
- o collection of payments and fees

- subsidy program accounting [USDA88]
- issuance of drivers and other licenses

b. Efforts at a federal employee ID card

Efforts are currently underway, through the Federal Smart Card Users Group (FEDSCUG), to explore the feasibility of a government-wide employee identification card. Such a card would replace the numerous cards and identifications that a government employee must currently carry to conduct business. Some of the issues being raised concerning government use of smart cards include: what fields or data elements should such a card contain as a minimum (i.e., minimal data set); what information should be optional (optional data set) and at the discretion of the issuing agency; what information is necessary to positively identify the bearer; what type of card is best suited for this application; do current industry and international physical card standards satisfy requirements; who has authority and responsibility for maintaining the accuracy and currency of card data; how and by whom are cards issued and retired, to what extent are cards issued by one agency acceptable by other government agencies; and what information should be human-readable versus machine-readable? In its simplest application the card would be a direct replacement to current government ID cards issued by each agency and would be used only for access to government buildings.

Such a government-wide card could enhance security of operations and reduce personnel, production, and equipment costs. By publishing the specifications for such a card, a larger and cheaper source of supply could be available than if each agency issued their own cards, each using different specifications. The Department of Labor is setting up a pilot project in its Washington, D.C. headquarters to evaluate the potential of a wider implementation.

c. Other efforts

The National Institute of Standards and Technology is currently investigating the use of smart cards to enhance the access control to computers and networks and the authentication of electronic funds transfers. For more information see [HAYK88].

3. Card and Token Activities in Other Sectors

It is in the financial and retail industries that we currently

see the largest use of these technologies: Types of ongoing activities include:

- o payment for products and services
- o storage of financial history information
- o recording of financial services transactions
- o access to account status information

Two other areas where these technologies are making inroads, and where use will likely increase substantially over the next few years are the health care and insurance industries. Applications there include:

- o storage of patient and health care history information
- o recording of medical and health care service delivery
- o processing of claims

In another area of the private sector, a joint venture by The Thomas Cook Group and SmartCard International Inc. uses the latter's UltiCard as a proprietary readerless card with its 64KB of programmable memory, aimed at the business and travel market. It is expected that the card will be used for such functions as recording expenses and electronic travelers checks, itinerary planning, hotel and airline preferences, user's personal profile.

Other application areas include medical (Methodist Hospital's Institute for Preventive Medicine, Baylor College of Medicine), educational (Robert Morris College, Chicago), home health care (InfoMed, Inc, Princeton, NJ), and insurance (Connecticut Mutual Life Insurance Co, Hartford CN).

4. Potential CALS Use of the Technology

"CALS encompasses the generation, access, management, maintenance, and distribution of technical data in digital form for the acquisition, design, manufacture, and support of weapon systems, ships and equipment." [OASD88] Its strategy includes: 1) standards, 2) technology development and demonstration, 3) weapons systems contracts and incentives, 4) DoD systems.

In Phase I, the emphasis of CALS will be on the delivery of engineering drawings and technical data in digital form. It is concerned with the generation, access, management, maintenance,

and distribution of that technical data as it supports the design acquisition, manufacture, and support of weapons systems, ships and equipment. Among the items included under technical data are:

- o engineering drawings
- o product definition and logistics support and analysis data
- o technical manuals
- o training manuals
- o technical plans
- o reports
- o operational feedback data

As CALS evolves, and its world becomes increasingly digitized and disbursed, it will be uneconomical and impractical for those who are contributing to its processes to deal with each other face to face. Under such circumstances procedures and techniques for affixing electronic digital signatures will be necessary. During all stages of a weapons systems acquisition and support life cycle, approvals and acceptances will be required. The use of biometric-supported smart cards can contribute to the integrity and confidence required of these processes. This is analogous to the use of this technology in the private sector for the transfer of funds and performing other financial transactions, which will also be of concern under CALS.

Under these conditions, it is likely that the primary use of card and token technologies in the CALS environment will be related directly to enhancing security. See below for a discussion of how these technologies can contribute to this end.

C. Computer Security Requirements, Features, and Issues

1. Overview

In dealing with these technologies, there is a general concept of "bearer" of the card or token and a "gatekeeper" to whom the card or token is presented, and who stands between the bearer and what's beyond the gate. [SVIG85] Much of the card technology is geared toward identification of the bearer and authentication that the bearer may perform a particular action. Among the security features and uses of smart cards are:

- personal identification
- access control to facilities and other resources
- access control to computer data and resources
- individual, workstation, process, communication, and transaction authentication; and affixing of digital electronic signatures to technical data products
- enhancing data integrity
- enhancing data privacy and confidentiality
- providing audit trails of access to sensitive data
- prevention of forgeries

The degree to which each of these security features and uses is a requirement of a particular application will affect the particular choice of card technology. In some cases, identification of the card bearer may not be important, only possession of the card being significant. This might be true in the case of a set of office workers sharing an embossed card that gives the bearer access to the unit's supply room. However, in sensitive applications, reflective of the CALS environment, there will be much more rigorous requirements.

2. Vulnerabilities of Smart Card Technology

Physical threats and vulnerabilities to smart cards include [SVIG85]: "internal card heating and heat dissipation, electronic static discharge, internal and surface conductor damage from bending and torsion forces, amateur experimentation on the electrical contacts and circuits." Put simply, a smart card may be subject to intentional or unintentional physical abuse. This is related to how people use the card or where its kept, as for example in someone's pocket or on a car dashboard in the sun. [SVIG85] lists an number of "other uses" for a card including as a: window scraper, shoe horn, door latch opener, toothpick, luggage tag, etc. To allow for this, one company issued a blank plastic card when it issued its FTC, hoping that its customers would utilize the blank card for these "other uses," thus sparing the FTC from damage.

In addition the threats and vulnerabilities related to physical conditions, the cards and tokens being discussed are subject to

being lost, stolen, or forged. However, in these circumstances it is really the security strengths of the card that are important. See the next section for a discussion of security strengths of smart card technology.

3. Security Strengths of Smart Card Technology

The basic security strength of a smart card stems from its architecture of supporting chips with their hidden areas that once initiated, cannot be read or altered. This read/write protection, guaranteed by the on-card microprocessor, is achieved either by allowing only the microprocessor to access the chip's memories or by requiring the use of some individual identification code for access by other sources. Further, this write once portion of the chip provides for the capability to maintain an audit trail of transactions and activities. Also, the chip's processor permits the encrypting of data and any password used as part of the authentication process. The chip is also capable of storing biometric data for use in identification of any user.

Therefore, in the case of the lost or stolen card, although an unauthorized person my physically have the card, use of it may be denied if that person does not know the correct encrypted password or does not have the matching biometric characteristic(s). (See below for a discussion of biometrics). There are two other aspects to a smart card that can be combined to provide additional security protection. The first is that a smart card has distinct memory zones. The second aspect is a feature that can render the microprocessor unusable when subjected to attempts at physical penetration of its data. Thus as a result of these security strengths, a lost or stolen smart card can be difficult or impossible to use, or forge, even if the unauthorized user or forger has a valid smart card in their possession.

4. Biometrics and Identification

The use of biometric data, in conjunction with having physical possession of a card, and knowing the correct combination of identifiers, passwords, and keys, makes user identification and authentication extremely reliable. Among the types of biometric data currently used are:

- o physiological attributes
  - digitized fingerprints

- hand geometry
- eye (retina) scans
- digitized photo ID

o behavioral

- keystroke dynamics
- voice verification
- signature dynamics

These biometrics can be used for both verification and recognition. Verification is where the system, utilizing the biometric information, verifies that there is agreement between the person making the claim and the biometric information supplied. Recognition is where biometric information is used as a template against a database of templates to identify an individual. An example of recognition is the use of fingerprints in a police environment. Although recognition may have some application in CALS, the use of biometric data on smart cards will likely primarily be for verification. See [MILL87] for a fuller discussion of the use of biometrics and smart cards.

5. Additional Issues for Smart Cards and Other Card Technologies

a. Individual responsibility and accountability

The use of card technologies for identification, access control, and authorization can additionally address and reinforce what is believed by many to be one of most significant pieces in the computer security picture, that of individual responsibility and accountability. Additionally, [HAYK88] notes that smart cards may be more secure because they are kept closer to the user, and thus may be more secure than a cryptographic device that they may replace.

b. Which technology is appropriate?

Each of the card technologies being discussed provides some means of protection with a certain cost associated with it. For some non-sensitive situations, a plastic card (without magnetic stripes, chips, or laser signatures) may be adequate. There are

those who believe that magnetic stripe cards with enhanced security features (such as a holographic imprint and laser signatures) provide sufficient economical functionality, capacity, and security for all but the most stringent environments, and that smart cards are costly "overkill." However, for the vast majority of CALS-related information, the variety and sensitivity of the data and resources will require that a high degree of protection be provided, thus perhaps mandating the use of technology such as smart cards.

c. Multiple applications

In a multi-application card or a single application card in which a number of different entities/people are involved (e.g., manufacturer, user application provider, etc.), who owns what and who has the right to what? These are issues of rights, privileges, and responsibilities that must be addressed.

VISA has recently announced their SuperSmart Card, a multiple application card that offers increased functionality - 16KB ROM, 8KB ROM, time, date, currency conversion, note pad, and two financial accounts - flexible film 16 digit liquid crystal display. It uses the DES when moving data. Power is supplied by an ultra thin film battery that is .5mm wide. VISA looks upon the SuperSmart Card as providing "improved risk control through self authentication, and improved customer convenience through self authorization."

This raises the issue of single versus multiple applications on a card. There are a number of affinity groups and vendors who would like to provide a set of related services using the same smart card. For example, in the context of the airlines, in addition to the credit card applications on the card, there could be reservations and ticketing, access to an airline lounge, special services in the lounge, etc. In addition, the card could be used as an emergency admittance to a medical emergency room. Any one of the cards' routine features could replace devices in which the feature is marketed separately (and perhaps at greater cost). In addition to the issues of rights, privileges and responsibilities mentioned above, there are technical concerns about how to keep the information separated, and how to give selective information access, that must be addressed.

d. The movement toward smart cards

The Electronic Funds Transfer Association in Washington, D.C. has forecast that there will be an average of 15 magnetic stripe cards per U. S. household by 1992. It is likely that the functions and features of the terminals that accept these cards

will keep pace with the proliferation.

Cards are used because: they are convenient, flexible, and economic; provide data security; and are necessary to support the volumes of traffic/transactions that society is generating. This is offset to some extent by the losses from fraud and abuse generated by illegal or improper use of these cards. Smart cards are an attempt to deal with the fraud and abuse problem. While from a technical standpoint smart cards can be effective, other factors that need to be considered in terms of their full acceptance and use include the huge installed based of magnetic stripe card terminals and equipment. It is expected that over the next three to ten years some of the economics related to the installed based of magnetic stripe equipment will shift, as a greater need for protection is perceived and as terminals and workstations that have the capability to read both magnetic stripes and chips are gradually installed. We are thus almost certain to see a phase-in type of transition, rather than a dramatic cutover in the private sector. However, in the CALS environment, the weight given to security factors is likely to skew the system requirements heavily toward the need for protection, rather than toward the preserving an installed base of hardware.

e. Single vs multiple chip cards

At the present time, in order to achieve increased capability, it appears to be cheaper and easier to design and produce a card with multiple simpler chips, rather than a single chip with the equivalent capability. However, there is a problem with inter-chip communications, resulting in security vulnerabilities. Single chip cards are thus far more difficult to penetrate since their memory buses are "buried within the chip's substrate and cannot be accessed without causing chip damage. Thus, the economy of using multiple chips could be out-weighed, in a CALS environment, by the need for more secure cards.

f. Distribution of sensitive material

Currently, a major concern of those directly responsible for computer security is the secure, reliable distribution of ID's, passwords, and cryptographic keys. Smart cards, single chip or multiple chip, may provide a safer distribution mechanism for these, since even if an unauthorized user gets access to a password, etc., without the appropriate smart card the unauthorized user is still prevented from accessing the system. Further, even if the unauthorized user has access to both the smart card and the appropriate password, application of biometric

information on the smart card (see previous paragraph titled "Biometrics and Identification") could still prevent access to the system.

g. Smart cards in a security program

[SVIG85 pp134-135] talks about "evolving a smart card security system to maintain" the following items in a "reasonable" way:

- o level of security
- o set of sensitivity tests for the unknown
- o set of back-up actions
- o understandable and implementable security plan
- o serious concern about the most dangerous participants-employees and customers
- o low cost of security that compares favorably with the risk
- o simple design that is acceptable as an international standard
- o transparent security process that is more difficult not to use

h. Authentication

In sensitive environments, authentication can be a two-way process of authentication of the user to the smart card and of the smart card to the user. Another issue is that if an authentication fails and the card "locks up" to prevent further intrusion, the user may not only lose access to the system, but may also lose access to the card and its data. This loss of card maintained data could be prevented if there is a way to get back into the card even if it has been "locked up." However, this ability to get back into the card creates the problem of possibly allowing an access route to the card data which could be utilized by an unauthorized party. Thus from a CALS security view, a decision must be made between possible loss of data versus possible unauthorized access. Also, once authentication takes place, it is necessary to maintain the security of the communication and transaction while it is still in progress. If encryption is used as part of the identification and authentication, it may introduce performance degradation depending how and where it is accomplished.

i. Effort to see what's on the card

In the case of embossed plastic, the information that is embossed is directly visible and can be easily read since it is almost always in plain text (i.e., not encoded or encrypted). In the case of magnetic stripe cards, the data is not directly visible, but it can be read with the proper equipment. In common usage, the data on magnetic strips is also not encrypted. With the use of smart cards, we begin to see significantly more effort required to read the data available from the card, at the same time, we also see a substantial increase in storage and processing capability.

j. Data Administration considerations

In the application of smart cards, Data and Database Administrators are presented with a tool that could help greatly in the protection of the data assets under their control. Working with security specialists, it may become possible for Data and Database Administrators to better control access to not only entire databases, but also to portions of any single database. For instance, it might be possible to encode into an individual's identifying smart card, what portions of multiple databases the individual is authorized to access. Thus, even if an individual gains access to an unauthorized password, he or she would still not be granted access to that portion of the organization's data assets since the needed access code has not been entered on his or her smart card. In order to make use of this type of capability, Data and Database Administrators must work very closely with security specialists to both develop the needed protections and to ensure that the protections are performing as required. No longer can Data and Database Administrators think of security as the single gateway that protects all of their data assets like a single locked door to a room. Instead, Data and Database Administrators must work with security specialists from the very beginning of the planning of any new or updated database so as to ensure that all needed security requirements are built into the database. Further, with smart card technology, Data and Database Administrators must also work with those security personnel responsible for management of access control, by providing up-to-date lists of which individuals are authorized access to what portions of the databases available on the system. Based on these lists, security would then issue the needed new or changed smart cards.

III. OPTICAL DISKS

A. Description of Technologies

1. Overview

This section discusses a variety of optical disk technologies. These are:

- o compact disk-read only memory (CD-ROM)
- o write once read mostly (WORM)
- o erasable
- o others

Among the features common to all is a surface of optically sensitive material in which tiny pits are cut into spiral or circular tracks that can be read by means of a laser beam. Each type of disk is capable of vast amounts of storage ranging in capacity from 200 megabytes to over a gigabyte (one billion) of digital data. It is these capacities, along with their compactness and portability, which allow for storage of, and access to, amounts of data that would otherwise be infeasible without this technology. The primary perspective taken in this section is the application of these technologies in conjunction with a personal computer or workstation. The degree to which each is viewed as a new tool and media for publishing or working with new material in new ways, or as a replacement for traditional magnetic storage technology, will depend on the characteristics of the technology and the requirements of each application. Each presents a number of potential information security opportunities. Below, each technology is briefly described, followed by a discussion of how CALS and others may use them, and the information security issues involved.

2. Compact Disk-Read Only Memory (CD-ROM)

CD-ROM is a read only disk system and is primarily a tool for publishing and information distribution and storage. Although WORM or erasable disk systems are commercially available, CD-ROM technology has progressed further in establishing a commercial market. It owes its origin to the CD-Audio products that have made large recent in-roads in the consumer marketplace. CD-ROM builds on the success of both personal computers and CD-Audio. In the case of CD-Audio, digitized audio is read and then

converted, with a digital-to-analog converter, to sound. In the case of CD-ROM, the digital-to analog converter has been removed and the digitized data, in the form of a bit stream, is fed directly to the personal computer, the same as if the data was coming from a magnetic disk.

The rigid disks, 4.72 inches in diameter, are made of a plastic base, covered by a material which can be stamped and read by laser beam. Finally, it is covered by a protective clear plastic coating, all of which makes the disk particularly rugged and resistent to a wide range of environmental conditions and physical abuse. In some of the newer CD-ROM drives, the disk must be placed in a protective cartridge before being loaded into the drive.

CD-ROM data is arranged in a continuous spiral track where equal lengths of track have equal amounts of data. Reading is done at a constant-linear velocity (CLV) by varying the rotation speed. This is as opposed to magnetic media, in which the data is arranged in concentric tracks, rotation speed is constant, and reading is done at a constant-angular velocity (CAV). The more complicated mechanism and slower access times (approximately 500 to 1,000 milliseconds versus 20-65 milliseconds) for CD-ROM is compensated for by its greater storage capacity - approximately 550 megabytes versus 360-1,024KB. One CD-ROM can be equated to approximately 1,500 360KB floppy disk, or over twenty-five 20 megabyte hard drives, or 250,000 pages of text. CD-ROMs are read 75 tracks per second, with each track containing 2,352 bytes with 2,048 bytes for data and 304 bytes for error detection and correction, and for addressing and synchronization. The effective transfer rate is 150 KB/second. It is significant to note that these design considerations were made to take advantage of what existed for CD-Audio.

Following a pre-mastering process in which the desired data is gathered, cleansed, formatted, tested against retrieval software, and prepared on a magnetic tape, a master platter is prepared. All of these steps, except for the preparation of the master, can now be done on cost-effective in-house workstations (costs of the workstations range from $30K to $50K+) or they can be done by a commercial service. From the master tape, disks are stamped out in a factory, the same manner as with CD-Audio disks since the processing facility does not distinguish what is being stamped out. Thus, the mass production techniques and economies of scale of the well developed, consumer-oriented, CD-Audio product are directly applicable to a computer environment.

Among the strengths of CD-ROM are [OLEA88]:

- it can be used to distribute very large databases
- it can enhance the availability of data
- it is cheap, light weight, portable
- it can simplify operations
- the read-only nature eliminates update synchronization and partial updates (with possibly higher data integrity)
- it reduces dependence on mainframes and networks and their related problems
- the disks are rugged
- the technology is readily available
- space efficiency of disks makes backups and archiving feasible
- with combinations of hardware and software the disks permit selective access to portions of the data
- the disks allow more opportunity for synergy by making it cost effective and easier to bring together different databases so that with artificial intelligence or other smart retrievals one can gain greater insight

On the downside [OLEA88]:

- more of the organization's information assets are concentrated on a piece of plastic and thus subject to compromise
- the concentrated assets may be quickly and easily distributed thus making them difficult to control

An advantage of CD-ROM over WORM and erasable media is that it has both physical standards (including dimensions, medium characteristics, and characteristics of the record and playback equipment), and logical format standards (including organization of the data into structures such as volumes, directories, and files). The physical standards were based on those developed by Philips (The Netherlands) and Sony (Japan) for CD-Audio. The

standards for audio are referred to as the "Red Book" and those for CD-ROM are referred to as the "Yellow Book." The logical format standards for CD-ROM file structure were developed by an ad hoc group, called the High Sierra Group (HSG), in May 1985 and the standard is now known as the High Sierra Group (HSG) proposal. Application level standards, which would define and interpret recorded information, have not yet been seriously addressed. For more information see [JANN87] [CDRO86] [ISO88].

A further degree of standardization is achieved with the release of Microsoft's CD-ROM extensions, which allows both CD-ROM developers and users to treat CD-ROM drives as standard MS-DOS peripherals. Drive vendors need only write their own device drivers.

Drives are available either as external units attached to a personal computer or as internal units, fitting into either full or half height disk drive slots. A large selection of vendors are now supplying CD-ROM drives. [TIAM88-2]

A very significant ingredient of CD-ROM's success is the retrieval software that has been developed as an integral part of this technology. Advances in database formatting, indexing, and retrieval software, along with their interfaces, permit real-time search of, and access to, all information on the entire disk. Search targets are usually specified as Boolean algebra combinations of given keywords. Retrievals are typically accomplished within a few seconds.

In some cases, the disk is used primarily for distribution of raw or nearly raw data with limited software and indexing. In other cases, value is added to the data by the vendor by means of user interface or retrieval software. In some recent developments, "intelligent" algorithms can be applied to improve the precision and recall of the user-specified search. The retrieval software, indices, and data structures, are elements that vendors use for product differentiation. However, despite the CD-ROM's large capacity, some applications do require proprietary compression techniques to minimize the required number of disks.

Although still trailing CD-Audio, price improvements are making CD-ROM systems increasingly attractive as potential standard personal computer peripherals. (CD-Audio players can be gotten for under $130 and disks in volume can be stamped for approximately $5; prices for CD-ROM drives are approaching $500 and lower, when purchased in volume).

CD-ROM technology is here today with a marketplace that many believe is beginning to reach critical mass in terms of the items

needed to cause an explosion in the number of users. Many of these needed items that are now in place are: drive and disk standards; greatly reduced costs for drives; low premastering, and production costs for disks; a growing proliferation of available titles; growing numbers of vendors resulting in a huge range of products and services; the growing sophistication of retrieval software; a rising awareness of the potential value of this technology due to the growing number of success stories and lessons learned.

3. Write Once Read Many Times (WORM)

WORM disks, like CD-ROM disk, store their data as pits in a recording surface. These pits, along with the flat areas between them, called 'lands,' are read by a laser beam attached to a mechanism that is capable of both course and fine tracking movements. The significant difference between CD-ROM and WORM disks is that on the WORM disk, a laser beam can also create the 'pits' or in other words, it can write to the disk. However, this writing process is not reversible, so that once written, the data becomes indelible. This data can be read many times, but it cannot be written over. New material to be added on the disk is simply written on an unused portion of the disk. Material that is to be logically deleted or replaced is not physically removed, but is flagged by the accompanying control software. This software flag is an indicator that tells the software reading the disk to ignore the data that has been logically deleted. With capacities of the magnitude of 200 megabytes to one gigabyte, this is a feasible approach for many applications. While different sized disks are available, 5.25 inch disk cartridges are tending to be favored, with storage capacities that are in the range of about 100 to 400 megabytes.

Two types of file structure are currently used on WORM devices, sequential files and linked files. The problem with sequential files is that they cannot be updated or extended, only copied. With linked files, each data block contains a pointer, so that old information can point to updated information. This method of storage provides the capability to update data with an audit trail. However, the price for this capability is that of degraded performance for each update. It is expected that improvements will continue to be made in techniques to conserve storage space, such as data compression and improving file and record update procedures.

WORM disks and drives are less standardized than CD-ROM, both in terms of physical characteristics (including size) and in terms of logical structure. Media and media format standards for 5.25

inch WORM devices are proceeding through the International Organization for Standardization (ISO) processes. One difficulty, however, is that there are two incompatible formats in the standards - "continuous" and "sampled," referring to the placement of data and servo tracks on the disk. There are also differences in recording and error correcting codes. The continuous format is more closely related to that used for magnetic disk and would appear to be more commercially practical. There is also some initial progress now being made in label and file structure standards for WORM devices. However, currently, WORM drives tend to be used in specific applications where the present state of standards can currently be overlooked. In the future, this may change as more standards in this area are accepted.

WORM systems are typically more expensive that CD-ROM systems, with drive costing about $5,000 and individual disks costing approximately $100.

4. Erasable

Erasable optical media is the least developed, least standardized, most costly of the optical products that are being examined. Like WORM, data is written with a laser beam in concentric tracks. However, unlike WORM, previously written areas can be erased and overwritten. Although other sizes are available, 3.5 inch disk cartridges will likely become increasingly popular.

There are three basic technologies that are competing in the erasable disk drive marketplace. One is dye-polymer technology which allows only a limited number of erasures. Tandy Corporation recently announced a personal computer based erasable optical disk product that would use this technology. It is not clear what impact, if any, the announcement will have in the near future. Another technology being pursued by Fujitsu is called phase change recording. It is likely that these two technologies will not be commercially available from multiple vendors in the near term. A third technology that is likely to prove significant much sooner is Magneto Optical (MO). Products using MO technology have been announced within the past year by a number of vendors. Additionally, some vendors have recently shifted their development efforts from WORM to MO products. MO media involves complex multilayer structures using transition and rare earth elements. Writing on an MO recording surface currently involves two passes, but one pass rewrite products are being developed. Access times are typically better than those for WORM drives and are comparable to many magnetic disk devices.

MO disks can be utilized just like magnetic disks since they can be rewritten as often as desired. Since the production process for MO disks is complex and costly, there is some question about their being manufacturable in large scale production quantities.

It would appear that, while it is not yet here in terms of readily available off-the-shelf products, erasable technology represents a future technology direction in terms of vendor development to satisfy the ever increasing user demand for relatively fast on-line storage. A number of users who do not need the audit capability of WORM, but who do need the storage, have indicated decisions to bypass WORM technology and wait until erasable technology is better developed, reliable, available, and cost effective. In the CALS Phase II and Phase III timeframes we will likely see the result of MO and other erasable disk developments, which promise to further close the gap between magnetic and optical disk storage systems. [KRYD87]

5. Other Products and Technologies

There are a number of related read only optical technologies similar to CD-ROM. They include Compact Disk-Interactive (CD-I) and Digital Video Interactive (DVI). These technologies share many format and other characteristic similarities. Although CD-ROM can carry any digital data, including representations of audio, graphics, and video, these other technologies are specifically oriented toward multimedia environments. For more information see [BREW87] [MASC88] [STRU88] [TIAM88-1].

A little further down the road is a related technology called 'digital paper'. This is a flexible plastic film that consists of a polyester-based fabric coated with a polymer dye that is sensitive to infrared light. The material, developed by ICI Electronics of London, can be cut into a variety of shapes and lengths, made into tapes, placed in cassettes, pressed onto disks, or cut into strips or tags. Data is stored by a laser beam which pushes aside the polymer dye to create spots. This technology achieves greater packing densities than has been achieved with rigid media. Capacities of one gigabyte per 5 1/4" disk and 600 gigabytes per 2400 foot reel are expected. These capacities combined with extremely low cost, for example half a cent per megabyte, and moderate access time of 40 milliseconds, make this medium potentially attractive. However, it is likely to be more sensitive to the effect of such things as surface dust, temperature, and humidity. Also, as with other new media, its archival qualities are undetermined at this point. The medium by itself does not appear to provide any special security and a user would have to rely on complementary technologies and

techniques such as encryption and access control software to protect sensitive information.

There are a number of manufacturers who are developing multifunction optical storage disks which include a combination of features from CD-ROM, WORM, and erasable technologies. The capacities, capabilities, and security issues, of each implementation is a function of which technologies are combined. See [DON087] for additional information.

B. Current and Potential Applications

1. Federal Agencies and the Private Sector

As we have seen, optical disk technology provides end users in government and in the private sector vast amounts of data (and storage), at a modest price. Further, for CD-ROM and WORM, this storage is in a format that cannot, through normal operation, be easily changed or destroyed.

a. The Private Sector

The private sector is increasingly recognizing the value of CD-ROM as a publishing medium. A sampling of current titles and subjects available on CD-ROM includes telephone directories, zip codes, bibliographies, abstracts, book indices, mapping information, encyclopedias, marketing, reference sets, medical and psychological information, scientific and engineering information, business filings, business and tax information, government regulation and information, and software. [TIAM87] [GARF88] Prices typically range from less than $100 for an individual disk, to several thousand dollars per year for a subscription. In some cases, the products represent versions of paper, tape, fiche or on-line offerings, usually with value added from associated indexing and retrieval software. In other cases, they represent new products.

CD-ROM is primarily a publishing and distribution vehicle. It is also used as a tool for training and as a medium for archiving. In some cases the organization publishes its own data, in other cases it publishes data belonging to another organization. Increasingly, organizations are turning to CD-ROM technology for internal distribution and use. Company regulations and procedures, training manuals, customer and client lists, field support manuals, underwriting and other decision rules, inventories, parts lists, and repair and maintenance manuals are examples. Hewlett-Packard Co., for example, has an HP LaserRom

project to distribute customer support documentation on CD-ROMS's.

A significant advantage of WORM systems is their very large capacity. Federal Express is using a graphics-intensive, interactive WORM-based system to train pilots to operate the company's Boeing 727's. The training system uses two video monitors to simultaneously display control and schematic images of 20 different airplane systems. [CUMM88]

Another application of WORM technology is data distribution. Account Line Financial Services of Jenkintown, PA uses it to distribute data on over 400 financial and demographic indicators to banks and other commercial clients. Triton Technology of Watsonville, CA uses WORM technology to collect deep sea mapping data for the National Oceanic and Atmospheric Administration (NOAA) and for its commercial clients (e.g., treasure hunters). Another application of WORM technology is the system being used by cancer surgeons at the Melanoma Center of the Robert Wood Johnson Medical School in New Brunswick, NJ to store pictures of lesions. The high storage capacity of WORM technology will allow the system to maintain, retrieve and archive this information for the large numbers of anticipated patients. [CUMM88]

b. The Federal Government

The federal government plays a number of roles with respect to optical disks since it is a major publisher and disseminator of information. In terms of CD-ROM, the government sells or makes available information typically in the form of paper or magnetic tape which others then repackage on CD-ROM for sale. A number of federal agencies are beginning to produce their own CD-ROMs for distribution. Others, are exploring the use of CD-ROM for their own internal uses. Some examples of government use of CD-ROM and government data on CD-ROM include:

- A number of firms produce disk titles on the scientific and technical publications of the National Technical Information Service (NTIS)
- The Census Bureau has recently produced a second demonstration disk of a variety of census data as it gears up to make major Census Bureau products also available on CD-ROM. A number of private companies now produce disks based on census data in which they provide added value with specialized search and display

software.

- NASA and the Jet Propulsion Laboratory currently have digital planetary data on 250,000 mag tapes; their goal is to produce an eighty volume set of CD-ROM's that contain all the prime planetary science data (using a compression ratio of 4 to 1 with decompression on the fly (real time)). There is currently an 11 volume set of CD-ROM disks available containing data from the Voyager flyby of Uranus.

- The Federal Deposit Insurance Corporation has problems with the distribution of the Uniform Bank Performance Ratios (UBPR), quarterly reports on 15,000 banks. In order to solve these distribution problems it plans to distribute these to 150 regional offices on CD-ROM. In another project, 25 million bytes of a rules and regulations database are being placed on a CD-ROM.

- One aspect of the Navy's Printing and Publishing Service (NPPS) move toward a "paperless ship" environment involves use of CD-ROM.

- DoD's Defense Logistics Agency (DLA) is working on a parts and logistics database as part of a major initiative called Fedlog (with CD-ROM disks replacing 100 microfiche) to automate the searching for and ordering of replacement parts.

- The US Geological Survey is utilizing CD-ROM as part of its technology transfer responsibility. It's National Earthquake Information Center has produced the first of six scheduled seismic event disks. Its Gloria disk with sonar images of the Gulf of Mexico is in final production; this is a joint project with NOAA and NASA to generate high resolution image displays on relatively inexpensive equipment.

- The US Postal Service handles 25,000 zip-code inquiries each day using a database of 25M data records covering 109M addresses in the national directory for 9 digit ZIP-codes, all in files on one CD-ROM; USPS is also considering making this application available to the public as user friendly screen formats are developed that would be easily usable by postal patrons without any training.

The Special Interest Group on CD-ROM Applications and Technology (SIGCAT), sponsored by the US Geological Survey, has been

particularly effective in bringing together government users and the vendor community to help the vendors better understand federal requirements, and to help government users to become more aware of available CD-ROM technology. Meeting announcements and minutes contain excellent overviews of what is happening in the federal and private sectors. [MCFA88] NIST, as co-sponsor with SIGCAT, hosts a CD-ROM demonstration laboratory at its Gaithersburg, MD facility where federal agencies can inspect a large range of commercially available CD-ROM disk drives and titles.

In terms of WORM technology, several large Federal government projects are utilizing this technology for data storage. The Internal Revenue Service is testing the use of a bank of WORM drives connected to a network file server to process Chapter 11 bankruptcy cases with an off-the-shelf document handling system replacing paper files. Among the largest federal WORM projects is the Patent and Trademark Offices's Automated Patent System which plans to place almost five million patent documents as digitized images on optical disk. The Library of Congress now has a system that stores about 400,000 document images on WORM disks and makes them available for public viewing. NIST is currently working with the National Archives to develop a method for testing optical disks to determine their suitability for extremely long-time storage of archivable information. [RIVE88] A variety of optical disk technologies are being investigated by NIST at its optical media laboratory in Gaithersburg, MD.

See [NADC86] for information on optical disk efforts in the defense community.

2. CALS and Optical Disks

The variety of optical disk systems will be very significant in the implementation of CALS. In digitizing the acquisitions and logistics processes, CALS will employ many and different types of vehicles for the storage and retrieval of many different forms of data.

The following are the system functions or technology areas used to categorize CALS projects: [OASD87]

- repository automation
- printing and publishing systems
- authoring systems

- database management and information processing systems
- communications access and data distribution
- presentation devices and maintenance aids
- automated procurement and parts control systems
- CAD/CAM and related tools
- system integration and architecture
- lead weapon systems demonstrations

Each of these categories requires retention of, and access to, large amounts of stored information. These retention and access demands for the data from these categories will result in system requirements that can quite possibly only be satisfied through use of some combination of the various optical technologies.

Based on current private industry and government applications, CD-ROM can be applied in CALS to the following kinds of activities:

- publishing and distribution
- a design and engineering aid
- a reference tool
- as an administrative and coordinating aid
- medium range and archival storage and as an aperture card replacement
- a training vehicle
- transaction auditing and other auditing

Among the type of items that are potential candidates for CD-ROM publication under CALS are: regulations, specifications, standards, engineering drawings, parts lists, inventories, design criteria, instructions, maintenance procedures, diagnostic protocols, and computer software. In some cases, the published material will directly support CALS applications. In other cases, it could be used as an aid in the administration of CALS and as an aid in coordinating among the various elements of CALS. Almost any reference material used by multiple participants in CALS is a candidate for CD-ROM use. These reference materials

could be developed by the government, they could be developed for the government by a contractor, or they could be purchased through a vendor or broker.

As CD-ROM and other forms of optical disk technology develop further, these technologies will be extensively used both as an aid to weapons designers and to train and help those who repair and maintain weapons systems. Later, in CALS Phases II and III, expert systems, with their needs for large knowledge bases, will also likely make extensive use of this technology.

In the future, archiving will depend heavily on the use of optical media. Any archiving application which currently uses magnetic tape, paper, aperture cards, or fiche is a potential candidate. Likewise, data which needs to be reviewed and analyzed by teams of people against specified criteria, as in the case of vendor proposals against Requests for Quotation (RFQ's) could be a candidate for placement on a form of optical disk technology. Certainly, any deliverable that requires multiple copies to multiple sources is an excellent candidate for placement on optical disk.

Since WORM disks are individually written rather than stamped or pressed, as in the case of CD-ROM disks, WORM systems would be most useful where there are large storage requirements, but where the numbers of copies is relatively small (one or a few). Potential CALS applications of WORM technology will include:

- o archiving of any of the variety of digital data which will be a part of CALS
- o floppy and hard disk replacements where large storage rather than speed, performance, or cost is the driving force
- o audit trails where maintaining a single indelible record of activities is important

Some organizations and vendors are using WORM devices as part of their in-house CD-ROM pre-mastering operations. In this case, the CD-ROM data, retrieval software, and indices are all developed and tested on the WORM device and then a production master tape is produced.

C. Computer Security Issues

As previously indicated, optical media will often be used with a personal computer or a workstation. In such cases, the security guidance issued for operating in these environments is

applicable. [STEI85]

In examining the security aspects of optical technologies, it is useful to remember that each characteristic can be viewed as either a strength or a weakness, depending upon your perspective. Thus the statement, "You can't write to the disk" could be viewed as either good news or bad news, depending upon your perspective.

1. CD-ROM

a. Security Strengths

The prime strength of CD-ROM from a security standpoint is that once it has been stamped it cannot be changed. Therefore, once the authenticity of the disk has been determined, disk integrity will be permanent and the user can have confidence that the disk contains the data that was originally placed on it.

Additional security advantages of CD-ROM, some of which are identified in [OLEA88], are:

- because the CD-ROM is read-only and is typically used at individual work stations, it avoids the problem of two users simultaneously accessing the same database
- identical copies of dated, newly mastered, entire disks can be distributed, avoiding the problems of partial updates
- high degree of data integrity since the data cannot be changed by overwriting it
- because of its large capacity, data intensive applications can be off-loaded and dependence on mainframe availability can be reduced
- a degree of freedom is achievable as network problems (and connect time and line costs) can be reduced
- physically, the disks are rugged, not subject to magnetic damage, and appear to have a long storage (shelf) life. Its stability and its environmental durability, contribute to making it a good archival media and therefore provide additional computer security
- it is more physically secure than magnetic media because the read/write heads can be positioned further away from the disk surface thereby reducing the

likelihood of head crashes

- drive and disks are readily available
- there is less need for users to get access to the mainframe, there to possibly 'browse' other files and non-related applications
- if the user application is not on-line, the dangers of line tapping and active interference is eliminated
- because of the nature of the media and its space efficiency, the archiving and sharing of large amounts of highly detailed backup data is encouraged
- with the appropriate retrieval and analysis tools, auditing functions that were previously infeasible can now be accomplished
- privacy of personnel notes can be achieved by retrieval software that permits the annotation of CD-ROM passages to be tied to the particular personal computer that is running the software
- it is more secure than other optical disk because a disk directory standard is in place [CDRO86]

b. Security Weaknesses

Despite its computer security strengths, CD-ROM has some drawbacks. The most serious is the degree of risk associated with having a vast amount of data concentrated and contained on a single disk, and thus subject to compromise all at one time. This means that greater access controls must be applied at the personal computer level and greater security awareness must be communicated to personal computer users. This awareness must include an understanding of the extreme importance of controlling distribution of disks, since even compromise of one disk could mean the loss of vast amounts of an organization's information assets. Under these circumstances, there needs to be a high degree of concern with the protection of: the workstations that use these sensitive disks; logical access to the information they contain; and their storage and disposal.

One vendor, Personal Library Software, has now announced a multifunction hardware/software system, ROI, to address some of the issues related to controlling access to a CD-ROM's data. Some of the security features of the system are: a secure audit trail of vital usage statistics; encryption of the CD-ROM's data;

selective access control; the ability to distinguish between browsing and downloading; and the capability to impose publisher or customer defined selective usage limits.

c. Some other CD-ROM security-related issues

The security of the mastering and production/manufacturing facility is of concern, especially if sensitive material is being processed. Currently only 3M Corporation claims to have a secure facility. This may change as the market for more specialized applications involving sensitive data grows. Also, many federal agencies are beginning to use CD-ROM to distribute data. In some cases, even though the data will be made public, the possible premature disclosure of time-sensitive data can be an issue to the publisher.

2. WORM

As a backup, WORM may not have the reliability and stability of magnetic tape. Currently people may have more confidence in magnetic tape for backup, and also drives and cartridges are cheaper for magnetic tape.

Another concern with WORM technology is how fast the optical disk gets filled up. For example, it costs approximately $125 for one 240M-byte optical cassette, which is a rather high price for that amount of storage capacity. Micro Design attacks the problem by combining use of magnetic fixed disk for interim updates with WORM disks then used for storage of final products. This raises the security question in this type of operational mode, what happens to an audit trail of the interim changes? Since, to date, there is no one agreed upon answer to this question, the consensus is that many system developers with large-capacity backup requirements will wait for erasable technology rather than go with WORM.

The availability of update audit trails on WORM disks can be of significant interest and worth to accountants, auditors, and security personnel. However, residual data that is flagged for logical deletion, but left physically intact, can be an unacceptable vulnerability to a user or an organization since once sensitive data has been placed on a disk it will remain and is thus still potentially accessible to an unauthorized person. Currently available WORM drives do not have the capability to physically destroy areas no longer being used. WORM disks contain toxic heavy metals which can create an environmental hazard unless the disks are left physically intact. Thus, destruction of classified material could prove to be a problem if

physical destruction is not allowed due to environmental issues. NIST researchers have invented a way to destroy data without physically destroying the WORM disk, but this requires a special provision when the media is manufactured.

Despite its audit trail capability, it is possible to make forged copies of WORM disks, as one could make forged copies of magnetic disks, by copying the entire disk while modifying the data as desired. One possible solution is having serial numbers stamped on the disks by manufacturers and the careful recording of these by users, all of which would serve to complicate the forgers task.

Like CD-ROM, WORM systems are rugged, durable and the disks appear to have a long shelf life, making WORM also a good archival media. This ruggedness also makes them ideal for environmentally harsh situations, such as battlefields. (See [SALT86] for additional information on design criteria.)

3. Erasable

Security concerns with erasable media are similar to those discussed under CD-ROM and WORM. Further, since the data stored on this form of optical media can be easily changed, it also has the same security concerns associated with magnetic media, only these concerns are multiplied due to the ability to concentrate even larger amounts of sensitive information on this form of media than can be done on magnetic media.

Like magnetic media, erasable optical media is subject to physical or logical erasures, or physical destruction. Thus, there is the need to back up the great volumes of data that can be stored on this media. Accordingly, either a large tape backup system, or a second optical disk drive, may be required for performing backup.

Also, like magnetic media, the method of erasure is important since there may be security vulnerabilities associated with data residue in which data is logically removed, but is not physically altered and is, therefore, still subject to compromise.

As with CD-ROM and with WORM systems, erasable disk systems may have excellent potential as archival media, and may be preferable to magnetic media where environmental conditions are harsh. (See section 4.j, Media stability, for additional discussion.)

4. Additional Discussion

a. Multiple applications, multiple users, and selective access

Currently, multiple applications on an optical disk are rare. A more common situation is one in which either there are multiple files on an optical disk or there are multiple users of the disk. Either situation may create a condition in which an individual has both physical and logical access to a disk, but is not authorized to access all parts of that data. For example, a CD-ROM publisher may include a number of book titles on a disk because it is economical to do so. However, the publisher may not want to give any one user access to all of those titles because of royalty or other pricing considerations. A number of retrieval software vendors are beginning to offer software or hardware and software blends that permit selective access control through some combination of:

- menu control
- hiding files
- password protection
- file encryption

As with protecting magnetic media, protection of the contents on an optical disk is difficult without some combination of both physical and software protection. One reason that physical protection is not sufficient is that once a CD-ROM is given to an individual who has a valid reason to access some portion of the content of the disk, use of DOS and other readily available utilities on a personal computer could allow that user to "browse" the disk and access unauthorized files. To solve this problem, it is possible to place protection-enforcing software on the CD-ROM itself, or on an accompanying floppy disk.

b. Other hidden data

In some cases, disk publishers have included test data and programs on production disks because it was cheaper and more convenient to master them that way. In the case of a CD-ROM disk, it is up to the person authorized to certify the master tape to determine to what extent such data is to be permitted and how should access to such data be limited. In some cases, sensitive data that was mastered onto the CD-ROM disk for economic reasons can be made unreadable by physically scratching out the undesirable portions.

c. Unforseen vulnerabilities

The optical technologies promise numerous potential applications while reducing or eliminating security exposures and vulnerabilities. It is expected that by 1990 there will be a $2.3 billion investment in CD-ROM, and there will four times as much spent on information as is spent on drives. [HELL86]

Optical media is more than merely a larger storage media as compared to magnetic disk. With optical media we cannot only expand the scale of what we are currently doing, we can manipulate data in new ways. The synergism created by being able to search large amounts of information from different sources begins to open up new ways of thinking about information. As with artificial intelligence, these new applications and processes may introduce new vulnerabilities, the specifics of which we don't yet know, but for which the user must still, nonetheless, be prepared.

d. Aggregation and inferencing

When large amounts of data are easily available, the concerns related to the potentials of aggregating information and thereby accessing sensitive/proprietary information are greatly expanded. Thus, the extensive storage capacity of optical disks, in conjunction with their ease and speed of access, multiply the problem of aggregation and inference.

e. More dependable than alternatives

Optical systems can avoid computer security problems related to loss of information that can occur when transferring information through use of other physical media. For example, the Pan American Health Organization distributes critically needed health information on CD-ROM to locations where the performance of other sources for distribution are marginal (rough handling destroys magnetic disks) or nonexistent (no communications lines). Also, as previously discussed, optical systems can be used to bypass a large range of other vulnerabilities associated with telecommunications.

f. Plagiarism assisted

Since data is relatively convenient to access on optical disk by using the appropriate retrieval software, plagiarism may be made easier. However, the same retrieval software may also be used as a tool for detecting such plagiarism.

If CD-ROM is to be used as a software distribution media, among other things, special protection will be necessary for commercial licensed software.

g. Media stability

The stability of CD-ROM, its environmental durability, and its expected long shelf life, contribute to making it a good archival media and thus provide additional computer security. Like CD-ROM, WORM systems are likely to be rugged and durable and to have a long shelf life, making them also a potentially good archival media and possibly suited for environmentally harsh situations, such as battlefields. (See [SALT86] for additional information on design criteria.) However, while systems purchased for the military have probably passed some testing, the large variety of recording techniques and chemistries make it difficult to apply lifetime data from one decoding method to another. Additionally, for military applications, there is uncertainty about the full effects of such things as pressurization/depressurization cycles, ionizing radiation, and electromagnetic pulse.

WORM and MO media have high raw data error rates compared to magnetic media. This requires the use of powerful, computationally intense error detection and correction routines. As the media ages, performance may become unacceptable. Such systems would require monitoring and automatic copying of the data to new media when some specific error level is reached, thus affecting considerations of media lifetime.

h. Disk authenticity and data integrity

Because WORM disks can only be written to one time, they are considered a valuable tool for audit trails and archiving. However, a threat still exists from a forged WORM disk in which some of the data has been copied intact, but in which some of the data has been deliberately altered. There needs to be a method for authenticating that a disk does, in fact, contain what the user expects it to contain. Perhaps due to the newness of this technology, there has so far not been much work done to address this problem. It is likely that research being done regarding authentication of financial transactions, access to computer systems, digital electronic signatures, and access to networks will be applicable. Of course, the authenticity of disks and data are also a concern with CD-ROM and erasable. (See section D.1, above regarding CD-ROM and [FIPS85-2].

i. Data Administration considerations

Since optical disk technology stores such a great amount of data in such a small physical volume, this technology will place a great amount of responsibility on Data and Database Administrators to ensure the protection of this data. While security specialists will have responsibility for the actual security mechanisms in use, it will be the responsibility of the Data and Database Administrators to ensure that all data that requires protection is protected. Further, it may be the responsibility of the Data and Database Administrators to segregate data between different optical disks in such a way as to minimize the impact of the loss of information on any one such physical device.

A further problem that Data Administrators must consider is that of data distributed by optical disk technology being used to achieve a mosaic effect by its recipients (see I.B.2, Data Protection). While this problem currently exists, it will be greatly magnified by the vast amounts of data that can be quickly and easily distributed by optical disk technology, such as a handful of CD-ROM disks. For example, Data and Database Administrators must now review the lists of recipients of CD-ROMs while considering not just the security level of the information on any one CD-ROM, but the possible aggregation of all the vast amounts of information an individual is to receive on multiple CD-ROMs.

IV. ARTIFICIAL INTELLIGENCE

A. Description of Technologies

1. Overview

This section addresses a set of technologies, collectively referred to as artificial intelligence (AI). The individual technologies that are discussed here are very different in what they are, what they attempt to do, and how they go about doing it. They all have, at their root, some concept of using a computer to mimic human behavior by performing in an "intelligent manner." Although there is no common agreement as to just what intelligence is, most views incorporate some notion of problem solving ability. [MINS86] The goal is to extend human problem solving capability through the use of a computer.

With regard to computer security, artificial intelligence can be a tool to assist in ensuring the confidentiality, integrity, and availability of our information systems and data. AI also represents a set of tools that will be increasingly applied to every aspect of our lives, and which presents potential vulnerabilities that its users must be aware of and address if the technologies are to satisfy their potential. For an overall perspective on the current status and future directions of AI, see [WALD88].

The major branches of AI are:

- expert and knowledge-based systems
- natural language interpretation and continuous speech recognition
- machine vision and robotics
- knowledge processing, cognition, pattern recognition, process control, neural networks

Each of these major AI areas is briefly described in the following section. This is followed by a look at how AI is being applied by others and how it might be applied by CALS. Finally there is a discussion of the information security issues related to the use of AI. Because of its advanced development and proliferation relative to other branches of AI, and because of its high potential for early impact on CALS, expert systems will be the primary focus of the discussion.

2. Expert or Knowledge-based Systems

The term expert or knowledge-based systems refers to a set of programming tools which allow the knowledge of an expert in a given field to be captured and applied by an automated system. Among the notions that it embodies are:

- emulates human expertise in a given domain
- makes logical deductions from given information
- uses the rules of logical inference
- performs convincingly as an advisory consultant
- provides self-explanation or lines of reasoning that led to decisions on demand

The basic components of a knowledge-based system are:

- a knowledge base of data and rules that are applied against the appropriate collection of data
- inference processing which applies the rules
- a human interface to the computer system that provides for user dialogue

Among the methodologies used for inference processing programming methodologies are:

- forward chaining (or goal-directed processing) in which the program proceeds from events, facts or assertions to possible outcomes, implications, or conclusions
- backward chaining (or data driven processing) determine what set of inputs, conditions, or circumstance would be necessary to achieve specified goals, outcomes, or hypotheses
- hybrid systems which combine elements of both forward and backward chaining

Unlike traditional programming languages, expert systems can:

- process rules of thumb, heuristics, and symbols

- be flexible and open-ended
- deal with uncertainty

Until recently, expert systems, and other branches of AI, belonged exclusively to the domain of mainframes. However, an increasing number of tools and systems are becoming available for personal computers and super personal computers. This trend will likely continue with advances in workstation hardware and expert system shells, i.e., software tools designed for developing expert systems. Among the languages for programming expert systems are Lisp, Prolog, OPS5, and C. See [CUGI87] and [BARB87] for additional information. An increasing number of personal computer based expert system shells are now available. See [CARA88] for more on AI sources.

3. Natural Language Interpretation and Continuous Speech Recognition

This branch of AI is devoted to the interpretation of written and spoken language by a computer. Much research is being done in university and intelligence environments in this area, but developments have not yet proceeded to large scale commercial applications. This set of technologies requires much computing power. Additionally, although progress is being made, many technical problems need to be solved before there is reliable, human-like understanding by a computer of written and spoken language. One area where attempts to use natural language developments are occurring is as "front ends" to other expert systems.

4. Machine Vision and Robotics

In this area of AI, the problem to be solved is how to imbue a machine with human-like vision and movement, with special emphasis on manufacturing. Many significant developments are taking place in this area. Japan, with its Fifth Generation projects, still maintains a lead in the application of this branch of AI. Efforts in this area are underway at NIST's Automated Manufacturing Research Facility (AMRF) in Gaithersburg, MD. [AMRF88] For more information see [FOLE87] and [ERIS87].

5. Knowledge Processing, Cognition, Pattern Recognition, Neural Networks

This area of AI seeks to better understand such things as the mind, the brain, and human intelligence. Knowledge gained from these studies are used to build computers that exhibit intelligent behavior. Neural networks attempt to pattern computer programs on digital models of the physical operations of the neural networks of the brain and the neural systems. After many years of being snubbed by the bulk of the AI community, there is a resurgence of activity and a number of real-world problems are being addressed, however, this branch of AI is still very much in its infancy.

B. Current and Potential Applications of Artificial Intelligence

1. Overview

Within just the last few years, AI, in general, and expert systems, in particular, have come out of the laboratory and the universities and have become a serious, "bottom line" tool of business and industry. Among the areas in which expert systems are now being employed are:

- quality control in manufacturing
- maintenance and diagnostics
- inventory control
- resource scheduling
- claims processing and insurance adjusting
- optimizing and customizing systems
- training

A sampling of AI applications in the government and in the private sector is offered below.

2. Private Sector Activities in AI

AI private sector activities include:

- Digital Equipment Corporation has developed and is using expert systems to help sales engineers order the right combination of components for VAX minicomputers

- Ford Motor Company is asking suppliers of automation equipment for their Factory of the Future to develop and supply expert systems to assist technicians to repair and maintain their gear

- the American Exchange uses expert systems for their credit analysis operation

- Evensky & Brown of Miami, FL is using their expert system for individualized financial planning

- Northrop Aircraft Division of Hawthorne, CA developed an expert system for process planning operations related to the manufacture of military aircraft where it may be necessary to exercise control over more than 10,000 individual parts

For additional discussion of these and other efforts see [DAVI87]. For a listing of some of the AI activities of a selection of major computer companies see [DAVI86].

3. Federal activities in AI

- a US Navy prototype called FRESH uses expert system and natural language technologies in the Pacific command to monitor fleet changes providing information on readiness operations and capabilities and how to respond to significant changes

- another Navy system, called CAT, is the first "on-board operational military piece of artificial intelligence software" and is used as a support tool assessing the stress on the vessel

- the Army Missile Command at Redstone Arsenal, GA is developing an expert system to provide a format for cataloging and using producability information, to help in training new engineers, and to increase the productivity of experienced engineers

- Martin Marietta is developing an expert system to perform knowledge-based risk management for the Department of Energy

- the Environmental Protection Agency is using expert systems to provide technical assistance for resolving resource intensive, technically complex problems. Addressing issues of water resources is one of the areas covered

- the Social Security Administration is developing an expert system for benefit claims processing

- the Army's Information Management Office is prototyping a expert system for document-tracking and decision support

- the Pittsburgh Research Center of the Bureau of Mines has developed three expert systems to advise on mining health and safety

- the Army Logistics Center in Fort Lee, VA has a full time group to produce expert systems; efforts include systems for intelligent computer-aided instruction for maintenance and diagnostics, office automation, and personnel requirements

- the National Ocean Service is exploring the use of expert systems for nautical charting

C. Potential CALS Applications that could Exploit AI

CALS will make increasing use of AI technology to address a variety of its activities and problems such as engineering design, test and evaluation, maintenance, training, and contract management. As with the rest of government and the private sector, it is likely that in the future there will be few data intensive activities that will not be touched by some aspect of AI.

In addition to the use of AI in mission-related and administrative and management functions, CALS will likely use AI to enhance the security of its processes. This may be done by using it to perform risk assessments; access control, identification, and authentication determinations; and by applying intrusion detection techniques. See below for a fuller discussion of computer security issues.

D. Computer Security Issues

1. AI as an Aid in CALS Information Security

a. Risk assessment

Risk assessment will be an important ingredient to the integrity of CALS. Risk analysis can be complicated, especially in high technology, widely distributed, diverse environments. Expert systems may be useful as aids in conducting the various risk analyses that will be required. Also, use of expert systems could result in increased uniformity in the performance of risk assessments. [MAYE88] describes an effort conducted for DOE to explore just such an application, and discusses the limitations of current personal computer based risk analysis products.

b. Access control and inferencing in multilevel environments

Multilevel environments, where some users are not cleared for the most sensitive data on the system, present difficult problems of access control. The implementation of formal access control models can be extremely complicated. In addition to keeping track of who has access to what data, the system needs to determine the likelihood of possible inference violation. In such a case, an authorized user can piece together or infer sensitive data through access to sets of non-sensitive data. Work is currently underway for the Air Force by SRI to study these problems. [LUNT85] [LUNT88-3] [MORG87]

c. Intrusion detection

If there is a violation of the system or data, a good security system needs to know that it has occurred, so that steps can be taken to recover from the intrusion and prevent reoccurrences. [LUNT88-1] [LUNT88-2] [MORG88-1] reports on the application of knowledge-based systems to this problem.

d. Decision tracking

Use of AI techniques may permit the tracing of the input to a decision, thus allowing for better decision making in the areas of reliability and maintainability of some specific resource. In fact, AI should prove applicable in many areas where the logic of the decision process needs to be traced and documented.

e. Monitoring

Expert systems could be developed to monitor various data

processing activities. Such expert systems would utilize decision rules for auditing, exception processing, and fraud detection. Issues which would have to be considered during the development of such expert systems would include types of rules, threshold levels, and tools for analysis.

f. Diagnostics

Another security application of expert systems is in their use in hardware and software diagnostics. These expert systems would not only help to solve specific problems, but the feedback they could provide to design engineers could then be utilized to improve various aspects of system security during the design phases of any new or upgraded software systems or hardware.

2. Security Strengths and Vulnerabilities of CALS AI Applications

a. Concentration of sensitive information and resources

A significant vulnerability in the use of expert systems is the fact that they bring together, at one logical location, a large amount of your organization's information and expertise. This presents a greater risk than if some unauthorized source were to get access to just an individual file. The expert system can tell an unauthorized person a great deal about an organization, including how the organization processes information in order to make decisions.

b. Integrity of our AI tools

The critical question that must be asked about AI tools is, how can it be determined that there aren't holes, intentional or otherwise, in the algorithms of an artificial intelligence process or expert system? To answer this question there is a need for test procedures and test criteria. The very size and complexity of an AI system may make it difficult or impossible to fully comprehend and test. While the same question could then be asked of processes that are not automated, the automation concentrates the resources, and intensifies the risk factors.

3. Other Issues

a. Protecting the AI System

In an AI system, we must not only be concerned about the

classification of data in our knowledge base, we must also be concerned about the classification of the rules in the AI system. The rules themselves must be appropriately classified and protected.

b. Testing security plans

AI could be used to test the completeness of not only computer security plans, it could also be used to test the vulnerabilities of other management plans and policy implementations as they relate to security.

c. Unanticipated attacks

While AI systems may be quite useful in exploring possible vulnerabilities associated with the application of certain security policies, an AI system applied as the actual system security mechanism may fall victim to, or not be sensitive to, any number of methods used to gain unauthorized access to a system such as overloading queues or otherwise causing the unexpected.

d. Detecting abuses

One of the chief vulnerabilities of any system is the attack by those who normally have legitimate access to the system. The CALS community can use card and token technologies combined with AI, in a manner similar to that of financial organizations, to look for differences in patterns of behavior. The AI system could then alert the appropriate parties as to the change in a user's behavior pattern that might signal an attack on the system. Research into application of AI techniques to the mosaic problem and intrusion detection problem are just in their infancy.

e. Data Administration considerations

The use of AI may prove to be the primary tool used by Data and Database Administrators in the fight to protect the data under their control from unauthorized use. As mentioned previously in this section, the application of AI technology may be quite useful in determining the possible potential of, and protecting against, data from various locations being combined in a mosaic effect.

Other Data and Database Administration areas of CALS in which AI and knowledgebased technology will prove quite useful include logical database design and physical database design and implementation. Use of AI technology during the design,

development, and implementation phases of a database should prove to be a great assist in attempting to ensure that all needed security aspects have been accommodated. However, the drawback to this area is that the knowledgebase of rules on which an organization's AI technology systems are built is, to Data and Database Administrators, a database requiring extreme care and protection.

V. TELECOMMUNICATIONS AND NETWORKING

A. Description of Local Area and Other Networks and Basic Taxonomy

1. Overview

In the previous sections we looked at individual technologies as applied to individual, possibly stand alone, computers with access only by other equipment of limited capability such as "dumb" terminals. This section takes the world view of nodes and networks and connections. It focuses on what needs to be communicated and what is the degree of sensitivity of that material. The world of telecommunications is extremely large and complex. Telecommunications will be integral to the success of CALS operations. The purpose of this section is to briefly indicate the ways in which CALS will use telecommunications and what some of the new technology related issues are that will have to be addressed. See [ABRA86] [BARK86] for more extensive coverage of the subject.

2. Some Basics

On one level, the concept of telecommunications is very simple. One party is logged on to a personal computer or workstation and needs to connect to another personal computer or workstation or database machine or mainframe resources - or to another person. [AMSE88] defines a telecommunications network as "the interconnection of systems and devices for the purpose of information communications." In the case of person-to-person communication, the connection can be at the same time, or one can leave a message or data for the other to be received or accepted at a later time. In general terms, connection might be sought for any one or a combination of the following reasons:

- o resource sharing
- o data sharing
- o direct, on-line communications
- o electronic mail or bulletin board use
- o gateway to other networks, resources, and data

In order for the communication to take place, there needs to exist a way to link together, or network, the two or more

communicating parties. This may be accomplished with a physical media such as conducting wire or a fiber optic or other type of cable, or it can be accomplished by a means of transmission, such as a private branch exchange (PBX), or a communications satellite. Of course, many networks utilize various combinations of these connection technologies. For information on the security of dial-up lines see [TROY86]. A type of connection that may be particularly important to CALS is that in which a limited number of people are connected to each other, along with their shared resources and gateways, over a limited geographic area (e.g., a building or a campus) on a local area network (or LAN).

Among the concerns of those using a LAN are:

- the availability of the connection or link
- that they can send and receive data easily and use the networks resources
- the integrity and confidentiality of transmission they send or receive
- that they know who they are communicating with, and that the person they are communicating with is authorized to take the action that they are taking
- that they have a means to provide positive identification of themselves
- what encryption techniques are employed

3. Other Telecommunications Services

In addition to accessing resources to which they are directly connected (hard wired), CALS and other government and contractor personnel may need to use services that are remotely located including electronic mail, bulletin boards, or on-line information, financial, or other services. In order to access these other services it would be necessary to allow some form of connection to be established with these other systems that might have no, or questionable, security practices. Thus, from a CALS perspective, the advisability of allowing communications to these services that are coming into existence because of various new communications technologies may, or may not, be acceptable under given circumstances.

B. Current and Potential Applications

There are a number of types of communications that might be required in the CALS environment. These (perhaps overlapping areas) include:

- o data, graphics, and text information (i.e., the actual application content - these can mostly be thought of as the content databases)
- o information about application data (formats, etc.). This type of information is referred to as "metadata"
- o administrative/operational communications
- o bulletins, emergency action notices, crisis management calls
- o electronic mail
- o procurement-related announcements, documents, inquiries, responses
- o access to remote information sources (vendor and information utilities)
- o design-related communications
- o test procedures, instructions, data, results
- o CALS committee communications including announcements, agendas, minutes, ballots

As the communications technology becomes more sophisticated and functional, there is likely to be more business transacted via conferencing in which those at remote locations can participate in discussions and the preparation of multi-authored documents. For further discussion of LAN and other networking applications see [BARK86].

C. Computer Security Issues

1. CALS Need for Telecommunications Security

The basic considerations for network telecommunications security will also apply in the CALS environment, but these considerations

are intensified. This is due, in part, to:

- o the sensitive nature of CALS data which can contain
  - a whole variety of information about current and future weapons systems and their deployment from which much 'intelligence' can be gleaned
  - procurement sensitive information
  - company proprietary information
- o the great geographic dispersion of the data and the large numbers of people, both in and out of government, who will have access to pieces of that information
- o the sheer magnitude and complexity of the CALS environment, which will make management and control a particularly challenging problem

2. Overall Network Security Responsibility

A number of issues arise with regard to the management and operation of individual CALS networks and the whole communications environment. These questions of responsibility include:

- o what types of communications will be permitted under CALS?; how will it be controlled?; what communications standards will be used and what communications software will be permitted/standardized upon?
- o what will be the management policies of the networks?; will each project/node have its own security officer?; to what extent will there be inter-service/inter-project communications?; will such communications be done with a common language?
- o when we are dealing in a communications environment, a concern is who provides what element of overall network security?; what is provided at the nodes, at the communications links, and at the individual workstation?; to what extent is this security proved by the communication software, by the operating system?; who is responsible for which link of the chain?; who, from an overall CALS perspective, is responsible to insure that nothing "falls through the cracks?"

- who is responsible for certifying that a network or node is secure?; will CALS develop standardized processes, tools, and techniques so that each vendor does not have to "reinvent the wheel" from scratch?

- encryption will definitely be necessary for some CALS-related communications - in such a situation, some of the technical considerations in the management of the encryption keys include:

  - whether the key is public or private
  - the cryptographic strength of the key
  - the speed of the encryption/decryption using the key and the algorithm
  - the flexibility of the key and algorithm
  - its interoperability
  - the integrity of the processes and the transmitted data

  will separate decisions on these item be made for all of CALS?

- who determines which are secure or insecure channels requiring some form of access mediation?; who determines whether a given system connected to a network should provide discretionary access control, where users, at their discretion say who can access the system, or mandatory access control where users and files have fixed security attributes that are used to determine access (either administratively or by the operating system according to fixed rules)

3. Additional Network Security Concerns

The following are some additional network security concerns:

- some of the things that a LAN may be vulnerable to, and that it requires protection from are:

  - passive and active line intrusion
  - an intruder masquerading as someone else by making personal computer board modifications or using

someone else's name

- an intruder obtaining physical access to the LAN

- o any time a personal computer on a network uploads or downloads a file, it is possible that trojan horses, worms, or viruses that can cause damage may be introduced [TIME88-3] [LUNT88-2]

- o in the case of communication line failures, alternative paths or backup and recovery procedures are normally in place; do these alternate paths, backups, etc. provide for security at the same level of trust as the primary system?

- o access control considerations can be a function of location and geographic concentration and disbursion; in what ways are they similar or different if access is to:

  - a stand-alone personal computer or workstation with a CD-ROM peripheral with sensitive information?

  - a personal computer or workstation connected to a LAN that may or may not have mail, file, print, or other resource servers?

  - a workstation connected to a remote host or information utility?

There are a number of basic security concerns related to a stand alone personal computer or a personal computer on a LAN or a personal computer or a workstation connected to a remote host via telecommunications. For a discussion of a personal computer in a stand alone environment see [STEI85]. For a discussion of dial-up communications, see [TROY86] [ZAJA88].

Many of the concerns noted above are shared among the various aspects of systems management. In the area of Data and Database Administration, those aspects that could either lead to unauthorized release of information from databases, or corruption of databases are the direct concern of Data and Database Administrators.

For additional information on telecommunications see [PARK88] [JOHN88] and [NCSC87-1]. Also see Section VI, New and Emerging Technologies and Standards, for information on telecommunications standards in place and under development.

VI. NEW AND EMERGING TECHNOLOGIES AND STANDARDS

From the outset, CALS has recognized the need for standards and specifications. [OASD88] describes the current standards and specifications which fall into the following basic categories:

- functional requirements standards
- data interchange standards
- data management and access standards
- communications protocols
- application guidance

In its incremental approach, CALS has required use of existing and emerging national and international standards. In the case of the technologies that we have been discussing, a number of actual and defacto standards exist. These have been discussed under the appropriate individual technologies. Some additional thoughts concerning new technologies and standards are presented below.

For identification cards, including financial transaction cards and integrated circuit cards (ICC's), there are standards and draft standards related to hardware and software interfaces, interoperability, and physical construction. Further, ISO is in the process of developing security architectures of financial systems using ICC's. Logical standards for the use of the chips' "real estate" have not been agreed upon. On the one hand, CALS should reap the benefits of a universally accepted card technology, but it needs to be clear when such acceptance is likely be achieved, and more importantly, whether the requirements of CALS will be satisfied by such standards. The CALS project is sufficiently large and its need for computer security sufficiently great that it may be able to directly utilize either existing or extended integrated circuit cards (smart card) standards. Additionally, working with other federal agencies, CALS could influence or help establish new defacto standards in this area. See [HAYK88 Appendix] for an overview of standards activities for integrated circuit cards.

In terms of CD-ROM, High Sierra Group and ISO 9660 do appear to be gaining a wide following, and there does not seem to be a major competitor in that arena. However, there are not as yet, standards regarding user interface to the variety of retrieval engines that are becoming available. The Air Force Acquisition

Office is trying to address the interface between the retrieval engine and operating system. The objective is to achieve at least some degree of compatibility across different disks running on the same drive. We are probably some time away from total hardware independence of disks. See [DISK88] for WORM and erasable defacto standards directions.

In the area of artificial intelligence, no one standard is emerging, primarily because different types of problems lend themselves to different tools. A number of expert system shells are now available on the market, see [PCWE88]. No one real leader is beginning to emerge yet, so depending on one product becoming universally accepted is risky.

There is considerable standardization work now underway in the area of telecommunications. The International Organization for Standardization (ISO) has developed a fundamental, multi-layered model of network architecture called the Open System Interconnection (OSI) basic reference model. It is being widely accepted as the future standard for communications networks.

Organizations and groups within the United States that are involved in telecommunications standards work include the American National Standards Institute (ANSI), the Manufacturing Automation Protocol/Technical Office (MAP/TOP), and the National Institute of Standards and Technology (NIST). NIST, through a set of implementors agreements on subsets of international standard protocols, established the Government OSI Profile (GOSIP). GOSIP is intended to promote multi-vendor interoperability through use of standards. GOSIP has been selected by the Defense Communication Agency, and it is required that Internet and the Defense Data Network (DDN) use GOSIP in order to transition to OSI protocols.

Using the OSI/ISO framework, DoD's Secure Data Network System (SDNS) project is promoting the design of the next generation of secure computer communications networks.

For additional information on standards efforts related to telecommunications and associated security issues see [BRAN88] and [KIRK88].

Except for the standards activities regarding integrated circuit cards, which come from a financial transaction heritage, the standards activities in this area have not especially focused on security.

In the Data and Database Administration area, the recent ANSI and FIPS approval of the Information Resource Dictionary System

(IRDS) Standard could prove quite useful in solving some of the problems these new technologies bring to this area. Due to the extensibility called for in the IRDS standard, CALS dictionary systems built on this standard could be easily modified by Administrators to carry the needed information to help attack the problems previously brought out in this document. For example, an IRDS based dictionary could be changed by its Administrator to carry information with every data element that identifies those other data elements with which it should never appear on the same physical device. These types of changes to an IRDS dictionary do not require any changes in the dictionary software, but are a natural provision of the extensibility specified in the standard.

VII. CONCLUSION

Information security is vital to the successful implementation of CALS. This report has addressed information security in the context of a number of new and emerging technologies which are likely candidates for use by CALS. Each technology has strengths and vulnerabilities with regard to information security. Each technology has a primary set of potential application. These potential applications by technology are:

- smart cards - personal identification, access control, and authentication
- optical media - publishing, database distribution, reference distribution, training
- AI - expert systems
- networking - access to remote data and resources

Use of these technologies may be necessary to achieve required levels of information security, or these same technologies may represent potential vulnerabilities that must be addressed. Knowledge about both information security and the new and emerging technologies is necessary for those engaged in CALS-related activities. Therefore, it is recommended:

- that CALS conduct an overall risk analysis; and develop both a global information security architecture and models by which those who have information security responsibility may be guided
- that these technologies and the information security implications of their use be explored in greater depth with a set of short term, specific objective pilot projects.
- that related information on technologies, tools, techniques, policies, procedures, and baseline standards and specifications with their increments be widely disseminated within the CALS community; that this distribution be in a user friendly, practical format (such as an information computer security CD-ROM) and that this distribution incorporate the information needed by CALS program managers, CALS Data and Database Administrators, and CALS contractors

As CALS moves towards a more digitized world, the legal status

of digitized records that replace hard copy is uncertain. Various forms of digital signatures to authenticate individuals, workstations, tokens, transactions, and processes will be required. This will pose both legal and technical challenges not only to CALS, but to the entire world.

Finally, in this report information security has primarily been addressed in the context of a number of new and emerging technologies. It is important to note, however, that no application of these new technologies changes the fundamental principle on which all security rests, that of individual responsibility and accountability. Since many of the new technologies discussed in this document increase dramatically the dangers of compromise or loss of large volumes of information, it is critical to develop an environment of trust and awareness that encourages the individual to be conscious about, and a willing participant in, protecting that information with which he or she has been intrusted. However, as this document also demonstrates, when utilized properly, these new technologies can also serve as excellent, and powerful automated tools, in the fight against loss or compromise of an organization's information resources.

BIBLIOGRAPHY AND REFERENCES

[ABRA86] Abrams, Marshall D. and Podell, Harold J., Computer and Network Security (Tutorial), IEEE Computer Society Press, Washington, DC October 1986.

[ALLEN] Natural Language Understanding, Allen, James, The Benjamin/Cummings Publishing Co., Inc., Menlo Park, CA.

[AMRF88] Automated Manufacturing Research Facility, NIST program description, October 1988.

[AMSE88] Amsel, Ellen, "Network Security and Access Controls," Computers & Security, February 1988, pp. 53-57.

[BARB87] Barber, Gerald, "The Lisp vs. C Debate," UNIX REVIEW, August 1987.

[BARK86] Barkely, John, Personal Computer Networks, NBS Special Publication 500-140, July 1986.

[BERS87] Berson, Thomas A. and Lunt, Teresa F., "Multilevel Security for Knowledge-Based Systems," published in the Proceedings of the 1987 IEEE Symposium on Security and Privacy, April 1987.

[BERS87] Berson, Thomas A. and Lunt, Teresa F., "Security Considerations for Knowledge-Based System," published in the Proceedings of the Third Expert Systems in Government Conference, October 1987.

[BERS87] Berson, Thomas A. and Lunt, Teresa F., "An Expert System to Classify and Sanitize Text," published in the Proceedings of the Third Aerospace Computer Security Conference, December 1987.

[BOWE88] Bowers, Richard, "Making a Living Off the Government," CD-ROM Review, January/February 1988, pp. 34-36.

[BRAN88] Brandstad, Dennis K., "Considerations for Security in the OSI Architecture, "Proceedings, 11th National Computer Security Conference, 17-20 October 1988, National Bureau of

Standards/National Computer Security Center, pp. 9-14.

[BREW87] Brewer, Bryan, "CD-ROM and CD-I," CD-ROM Review, June 1987, pp. 18-25.

[BREW88] Brewer, Bryan, "Still Waiting For "It" To Happen," CD-ROM Review, January/February 1988, pp. 15-19.

[CACI] CACI, Forecast, Assessment, Recommendations, Department of the Air Force, Computer-Aided Acquisition and Logistics Support (CALS), draft report, Andrews, AFB, MD 20334, undated.

[CALS88] CALS Industry Security Task Group Meeting Introduction notes, August 24-25, 1988.

[CARA88] Carande, Robert, "Checking Out AI Sources," AI Expert, Vol. 3 No. 6, June 1988, pp. 60-65.

[CAUD88] Caudill, Maureen, "Neural Networks Primer Part III," AI Expert, Vol. 3 No. 6, June 1988, pp. 53-59.

[CDRO86] "Working Paper for Information Processing - Volume and File Structure of Compact Read Only Optical Discs for Information Interchange," "Working Paper for a Standard CD-ROM Volume and File Structure," "Working Paper of the CDROM Ad Hoc Advisory Committee, May 28, 1986.

[CSA88] Computer Security Act of 1987, Public Law 100-235, January 8, 1988.

[CGO86] Electronic Collection and Dissemination of Information By Federal Agencies: A Policy Overview, 28th Report by the Committee on Government Operations, April 29, 1986, U.S. Government Printing Office, 58-206 O, Washington, DC 1986.

[COUR88] Courtney, Robert H., Jr., "Some Informal Comments About Integrity and the Integrity Workshop," Informal paper circulated for comment, Port Ewen, N.Y., September 1988.

[CSI87] 1987 Computer Security Buyers Guide, Computer Security Institute, Northborough, MA 01532, 1987.

[CUGI87] Cugini, John V., Programming Languages for Knowledge-Based Systems, NBS Special Publication 500-145, February 1987.

[CUMM88] Cummings, Steve, "Optical's Vast Expenses," PC Week, March 15, 1988, pp. s/17-18,22.

[DAVI86] Davis, Dwight B., "Artifcial Intelligency Enters the Mainstream," High Technology, July 1986, pp. 16-23.

[DAVI87] Davis, Dwight B., "Artifcial Intelligency Goes to Work," High Technology, April 1987, pp. 16-27.

[DENN87] Denning, Dorothy E., Neumann, Peter G. and Parker, Donn B., "Social Aspects of Computer Security", Proceedings, 10th National Computer Security Conference, 21-24 September 1987, National Bureau of Standards/National Computer Security Center, pp. 320-325.

[DENN88] Denning, Dorothy E., Lunt, Teresa F., Schell, Roger R., Shockley, William R., Heckman, Mark, "The SeaView Security Model," published in the Proceedings of the 1988 IEEE Symposium on Security and Privacy, April 1988.

[DISK88] 1988 Disk/Trend Report, Optical Disk Drives, DISK/TREND, Inc., Los Altos, CA, July 1988.

[DOD-1] Industrial Security Manual, DoD 5220.22-M, undated.

[DOD-2] Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments, CSC-STD-004-85, undated.

[DOD-3] DD Form 254, DoD Contract Security Classification Specifications, undated.

[DOD85-1] Department of Defense Trusted Computer System Evaluation Criteria, ("Orange Book"), Department of Defense Standard DOD 5200.28-STD, December 1985

[DOD88] DOD, CALS Implementation Guide, DRAFT MIL-HDBK-CALS, 29 January 1988.

[DONO87] Donohue, James F., "Optical memory goes multifunction - at last," Mini-Micro Systems,

March 1987, pp. 41-45.

[ELME88] Elmer-DeWitt, Phillip, "Invasion of the Data Snatchers!," Time, September 26, 1988, pp. 62-67.

[ERIS87] Erisman, Albert M. and Neves, Kenneth W., "Advanced Computing for Manufacturing", Scientific American, October 1987, Volume 257, Number 4, pp. 162-173.

[FCW88] "Executive Tech Briefing: CD-ROM Technology", Federal Computer Week, May 9, 1988, pp. 26-31.

[FIPS88] Data Encryption Standard (ANSI X.3.92-1981/R1987) FIPS PUB 46-1, National Bureau of Standards, January 1988.

[FIPS85-1] Standard for Password Usage, FIPS PUB 112, National Bureau of Standards, May 1985.

[FIPS85-2] Standard on Computer Data Authentication, FIPS PUB 113, National Bureau of Standards, May 1985.

[FOLE87] Foley, James D., "Interfaces for Advanced Computing", Scientific American, October 1987, Volume 257, Number 4, pp. 126-135.

[FOX87] "Advanced Computer Architectures", Fox, Geoffrey C. and Messina, Paul C., Scientific American, October 1987, Volume 257, Number 4, pp. 66-74.

[GARF88] Garfinkel, Simson, "Evaluating 12 discs for Libraries,", CD-ROM Review, July 1988, pp. 30-35.

[GASS88] Gasser, Morrie, Building a Secure Computer System, Van Nostrand Reinhold Company, Inc., New York, N.Y., 1988.

[GELE87] Gelernter, David, "Programming for Advanced Computing, Scientific American, October 1987, Volume 257, Number 4, pp. 90-98.

[HAYK88] Haykin, Martha E. and Warnar, Robert B. J., Smart Cards and Computer Security, draft NBS Special Publication 500-157, 1988.

[HELL86] Helliwell, John, "Optical Overview: What's Coming in CS-ROMs and WORMs," PC Magazine, October 14,

1986, pp. 149-164.

[HEND88] Guide to Information Resource Dictionary System Applications: General Concepts and Strategic Systems Planning, Margret Henderson Law, NBS Special Publication 500-152, April 1988.

[HIEB88] Hiebert, Lindsay, " AI and Network Planning," AI Expert, September 1988, pp. 26-33.

[HUT87] Hut, Piet and Sussman, Gerald Jay, "Advanced Computing for Science", Scientific American, October 1987, Volume 257, Number 4, pp. 144-153.

[IARF86] Emerging Technologies and Auditing: The Impacts on Future Audit Practices and Productivity, based on the 1986 Advanced Technology Forum sponsored by The Institute of Internal Auditors Research Foundation, May 5-6, 1986, Orlando, FL.

[INFO88] Neural Networks, Computers in Science, Info World Target Edition No. 1, appx 3/88 undated.

[ISO88] ISO 9660 Information Processing - Volume and File Structure of CD-ROM for Information Interchange, 1988

[JANN87] Jansson, Peter, "Patterning CD-ROM," PC Tech Journal, July 1987, pp. 163-173.

[JOHN88] Johnson, Howard L. and Layne, J. Daniel, "A Mission-Critical Approach to Network Security, "Proceedings, 11th National Computer Security Conference, 17-20 October 1988, National Bureau of Standards/National Computer Security Center, pp. 15-24.

[KAHN87] Kahn, Robert E., "Networks for Advanced Computing", Scientific American, October 1987, Volume 257, Number 4, pp. 136-143.

[KARN86] Editors: Karna, Kamal N., Parsaye, Kamran, Silverman, Barry G., Assoc Ed, Briscoe, Duke P., Oct 22-24, 1986, Tysons Westpark Hotel, Mc Lean Virginia, IEEE Computer Society Press, Expert Systems in Government Symposium.

[KIRK88] Kirkpatrick, Kimberly E., "Standards for Network Security," Proceedings, 11th National Computer

Security Conference, 17-20 October 1988, National Bureau of Standards/National Computer Security Center, pp. 201-211.

[KRYD87] Kryder, Mark H., "Data-Storage Technologies for Advanced Computing, Scientific American, October 1987, Volume 257, Number 4, pp. 116-125.

[LIEB87] Liebowitz, Jay, "Expert Systems for Business Applications," Applied Artificial Intelligence, Volume 1, Number 4, 1987, pp. 307-313.

[LONG87] Longley, Dennis and Shain, Michael, Data & Computer Security, Dictionary of standards, concepts and terms, Stockton Press, New York, N.Y. 10010, 1987.

[LUNT] Lunt, Teresa F. and Thuraisingham, Bhavani M., "Security in Large AI Systems," undated.

[LUNT85] Lunt, Teresa F. and Whitehurst, R. Alan, The Seaview Formal Top Level Specifications, A004: Interim Technical Report, prepared by SRI International for (prepared for USAF, Rome Air Development Center, Griffis AFB, N.Y. 13441-5700, Contract No. F30602-85-/c-2043.

[LUNT88-1] Lunt, Teresa F., "Access Control Policies: Some Unanswered Questions," Computer Science Laboratory, SRI International, Menlo Park, CA 94025, internal paper, June 3, 1988.

[LUNT88-2] Lunt, Teresa F. and Jagannathan, R., "A Prototype Real-Time Intrusion-Detection Expert System," published in the Proceedings of the 1988 IEEE Symposium on Security and Privacy, April 1988.

[LUNT88-3] Lunt, Teresa F., Schell, Roger R., Shockley, William R., Heckmanm, Mark, Warren, Dan, "A Near-Term Design for the Sea View Multilevel Database System," published in Proceedings of the 1988 IEEE Symposium on Security and Privacy, April 1988.

[LUSH88] Lusher, Elaine, "An Expert System for Logistics Management," AI Expert, September 1988, pp. 46-53.

[MASC88] Mascioni, Michael, "CD-I in the Business Market," CD-ROM Review, January/February 1988, pp. 28-30.

[MAYE88] Mayerfield, Harold N., Baltimore, MD and Troy, Gene, Denver CO, An "Expert System to Perform Knowledge-Based Risk Management, Center for Computer Security News, July 1988, pp. 19-25.

[MCFA88] McFaul, Jerry, meeting announcements and minutes, Special Interest Group on CD-ROM Applications and Technology (SIGCAT), sponsored by the US Geological Survey, 1986-1988.

[MCIV85] McIvor, Robert, "Smart Cards," Scientific American, November 1985m pp. 152-159.

[MEIN87] Meindl, James D., "Chips for Advanced Computing," Scientific American, October 1987, Volume 257, Number 4, pp. 78-88.

[MILL88] Miller, Benjamin, "Status of Security and Biometics," Security, Standards and Biometrics, Proceedings of Smart Card Applications and Technologies Conference, SCAT '87, Volume 3, The Information Exchange, Falls Church, VA, 1988, p.11-45.

[MINS86] Minsky, Marvin, Societies of the Mind, Simon and Schuster, New York, N.Y., 1986.

[MIS] The MIS Information Security Resource Manual, MIS Training Institute.

[MORG87] Morgenstern, Matthew, "Security and Inference in Multilevel Database and Knowledge-Base Systems," Proceedings, ACM International Conference on Management of Data (SIGMOD-87), San Francisco, May 1987.

[MORG88-1] Morgenstern, Matthew, "Constraint-Based System: Knowledge About Data," Proceedings, Second International Conference: Expert Data Base Systems, 1988.

[MORG88-2] Morgenstern, Matthew, "Controlling Logical Inference in Multilevel Database Systems," Proceedings, IEEE Symposium on Security, April 1988.

[NADC86] Proceedings of the Optical Memory Technology Review, Volumes 1, 2, and 3, Naval Air Development

Center and National Bureau of Standards, Gaithersburg, MD, June 11-12, 1986.

[NBS88] Computer Security Publications, NBS Publications List 91, July 1988.

[NCSC87-1] Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria Evaluation Criteria, ("Red Book"), National Computer Security Center NCSC-TG-005 Version-1, July 31, 1987.

[NCSC87-2] IIS Bibliography: A bibliography of materials relating to information security, NCSC publication, December 17, 1987.

[OASD87] CALS, Computer-Aided Acquisition and Logistic Support, (Report to the Committee on Appropriations of the United States House of Representatives, Office of the Assistant Secretary of Defense (Production and Logistics) Washington, D.C., June 30, 1987.

[OASD88] CALS, Computer-Aided Acquisition and Logistic Support, (Report to the Committee on Appropriations of the United States House of Representatives, Office of the Assistant Secretary of Defense (Production and Logistics) Washington, D.C., July 31, 1988.

[OLEA88] O'Leary, John G., "CD-ROM and Security...New Technology, New Problems, New Solutions," Computer Security Newsletter No. 80, January/February 1988, pp. 1-2.

[OMTR86] Optical Memory Technology Review Presentation Material, Organized by the Naval Air Development Center, Hosted by National Bureau of Standards, Gaithersburg, MD June 11-12, 1986.

[OSTP87] Executive Office of the President, Office of Science and Technology Policy, A Research and Development Strategy for High Performance Computing, November 20, 1987.

[OTA] Government Information Technology: Management, Security, and Congressional Oversight, OTA Report, undated.

[OTA85] Federal Government Information Technology:

Electronic Surveillance and Civil Liberties, U.S. Congress, Office of Technology Assessment, OTA-CIT-293 (Washington, DC: U.S. Government Printing Office, Oct 1985, p. 72.

[OTA86] Federal Government Information Technology: Electronic Record Systems and Individual Privacy, U.S. Congress, Office of Technology Assessment, OTA-CIT-296 (Washington, DC: U.S. Government Printing Office, Jun 1986, p. 72.

[OTA86] OTA Project Proposal on New Communications Technology: Implications for Privacy and Security, scheduled for delivery 9/86.

[OTA87] The Electric Supervisor: New Technology, New Tensions, U.S. Congress, Office of Technology Assessment, OTA-CIT-333 (Washington, DC: U.S. Government Printing Office, September 1987, p. 139.

[PARK88] Parker, T. A., "Security in Open Systems: A Report on the Standards Work of ECMS's TC12/TG9," Proceedings, 11th National Computer Security Conference, 17-20 October 1988, National Bureau of Standards/National Computer Security Center, pp. 38-50.

[PCIE] The Development of Standardized Computer Matching Formats, report from the Long Term Computer Matching Project and the Payment Integrity, report from the Project of the President's Council on Integrity and Efficiency (PCIE), undated.

[PCWE88] "Artificial Intelligence/Expert Systems Buyer's Guide - Expert System Shells," PC Week, February 1988, pp. 62-65.

[PELE87] "The Next Computer Revolution", Peled, Abraham Scientific American, October 1987, Volume 257, Number 4, pp. 57-64.

[REGA88] Regan, Priscilla M., Winston, Joan D., Electronic Delivery of Public Assistance Benefits: Technology Options and Policy Issues, Background Paper, U.S. Congress, Office of Technology Assessment, Background Paper OTA-BP-296 (Washington, DC: U.S. Government Printing Office, April 1988, p. 40.

[RENN87] Rennels, Glenn D. and Shortliffe, Edward H., "Advanced Computing for Medicine", Scientific American, October 1987, Volume 257, Number 4, pp. 154-161.

[RIVE88] Rivenbark, Leigh, "Optical Fileing Arrives: Agencies face the document image challenge," Federal Computer Week, July 11, 1988, pp. 27-28,34,36.

[RUTH88] Ruthberg, Zella G., Fisher-Wright, Bonnie, Perry, William E., Lainhart, John, Cox, James G., Gillen, Mark, and Hunt, Douglas B., Guide to Auditing for Controls and Security: A System Development Life Cycle Approach, NBS Special Publication 500-153, April 1988.

[SALT86] Saltzman, Marc, "Interpretation of US Department of Defense Specifications for Device Designers," Proceedings of the Optical Memory Technology Review, Volume 1, Naval Air Development Center and National Bureau of Standards, Gaithersburg, MD, June 11-12, 1986, pp. 111-126.

[SCAT88] "First Responses to the VISA SuperSmart Card," SCAT News, July/August 1988 p. 4.

[SEYM87] Seymour, Jim, "Artificial Intelligence: From academia to corporate America," Today's Office, November 1987, pp. 31-34.

[SMAR88] Special Issue on Health Care, Smart Card Monthly, Smart Card Concepts, February 1988.

[SNWS86] System Decision Paper (SPD) for Milestone IV Shipboard Non-Tactical ADP Program II (SNAP II), Snap Program Directorate, Space and Naval Warfare Systems Command, Washington, D.C., May 1986.

[STEI85] Steinauer, Dennis D., Security of Personal Computer Systems: A Management Guide" NBS Special Publication 500-120, National Bureau of Standards, January 1985.

[STRU88] Strukhoff, Roger, "CD-I, DVI, and You and I," CD-ROM Review, January/February 1988, pp. 22-26.

[SUMM87] Summers, Rita C. IBS Los Angeles Scientific Center

and Kurzban, Stanley A., and Stanley A. Kurzban, IBM Data Systems Division, Potential Applications of Knowledge-Based Methods to Computer Security, Los Angeles Scientific Center Report No. 1987-2814, Los Angels, CA.

[SVIG85] Svigals, Jerome, Smart Cards: The Ultimate Personal Computer, Macmillian Publishing Company, New York, 1985.

[TIAM87] Tiampo, Janet, Compiler "CD-ROM Disc Titles," CD-ROM Review, May/June 1987 pp. 45-48.

[TIAM88-1] Tiampo, Janet, "Taking Aim to CD-I," CD-ROM Review, January/February 1988, p. 25.

[TIAM88-2] Taimpo, Janet M., Compiler, "30 Business Applications on CD-ROM," CD-ROM Review, September 1988, pp. 54-55.

[TIME88-1] "Fast and Smart, Computers and the Future," Time, March 28, 1988, pp. 52-58.

[TIME88-2] "Putting Knowledge to Work, Computers and the Future," Time, March 28, 1988, pp. 60-63.

[TIME88-3] "Invasion of the Data Snatchers!," Time, September 26, 1988, pp. 62-67.

[TIPT88] Tipton, Hal, "NEW SECURITY NEED: Dial-up Access Control in an Era of Connectivity," Summary of Papers To Be Presented at the Eleventh Computer Security Group Conference, Kansas City, MO, May 3-5, 1988.

[TIPT88] Tipton, Hal, Rockwell International, "New Security Need: Dial-Up Access Control in an Era of Connectivity", Center for Computer Security News, July 1988, pp. 9-14.

[TROY86] Troy, Eugene F., Security of Dial-up Lines, NBS Special Publication 500-137, May 1986.

[USDA88] Peanut Buying Point Automation Project, 1987 Evaluation, United States Department of Agriculture, Agricultural Stabilization and Conservation Service, 1988??

[WALD88] Waldrop, M. Mitchell, Man-Made Minds: The Promise

of Artificial Intelligence, Walker and Co., New York, NY, 1988.

[ZAJA88] Zajac, Bernard P., Jr., "Dial-up Communication Lines: Can they be secured?," Computers and Security, February 1988, pp. 35-36.

[ZEMP86] Zempolich, Bernard A., "Optical Memory Storage Requirements and Applications for Use in Military Environments," Proceedings of the Optical Memory Technology Review, Volume 1, Naval Air Development Center and National Bureau of Standards, Gaithersburg, MD, June 11-12, 1986, pp. 19-92.

DATA MANAGEMENT

Information Resource Dictionary System: An Integration Mechanism for Product Data Exchange Specification

CALS SOW TASK 4.1.2.1

Information Resource Dictionary System: an Integration Mechanism for Product Data Exchange Specification

INTRODUCTION

This paper discusses the need for a mechanism that allows various views of product data to interface with various techniques for managing product data. The Information Resource Dictionary System (IRDS) [ANSI Standard X3.138-1988] is proposed as an integration and configuration management mechanism for the Product Data Exchange Specification (PDES).

BACKGROUND

The design of manufacturable products is an increasingly complex process for industry. Advances in technology have resulted in compartmentalized life-cycle product development activities. This has led to the isolation of the product designer from others participating in product development. Those isolated from access to the designer are: (a) the sponsor who has the need for the product, (b) the process planner who understands how the product can be produced in the factory, (c) the manufacturing manager who understands the operation and performance of the shop floor equipment, (d) the quality assurance inspector who understands how to measure the functionality of the product, (e) the service engineer who is responsible for repair and preventive maintenance of the product, and (f) the reliability engineer who is responsible for tracking the performance of the product over its lifetime.

At each stage of the life-cycle, important knowledge about the product is acquired. Unfortunately, this information is seldom available to staff working on other stages of product development. Specifically, the designer may not understand the impact of his design on the creation of a true 'world-class' product -- one built to minimum cost with highest quality and greatest functionality, in the shortest time span. To integrate the isolated activities of product development, more attention needs to be paid to the information exchange that occurs during the product life-cycle.

With sophisticated and ever evolving technologies, users of product data are faced with the need to exchange information across diverse and dissimilar systems. At the same time, these users must maintain the various contexts within their organization and functional responsibility. The integration of systems as well as the integration of information within this technological heterogeneity is the "core" of the developing Product Data

Exchange Specification (PDES). Recognition of the need to organize the integration and exchange of this information has resulted in a major effort within the PDES community to define an architecture for this purpose.

TOPICAL MODELS

The PDES community has been seeking solutions to manage and exchange information about products as opposed to the graphical exchange of drawings of products. The IGES/PDES Organization, voluntary standards organization, has been developing the product information descriptions (called conceptual models) across a broad industrial base (e.g. mechanical, electrical, etc.). These descriptions, some common to many industries and some unique to particular industries, form a "core of information" about products. As application activities are defined, committees have been formed to formalize the necessary information shared between product development activities. This effort has resulted in conceptual models which provide the framework for the product information to be exchanged.

When a consensus has been reached on an individual topical model, the model is then voted out of committee as a draft specification. The various models have then been considered for integration, when they contain common information. The PDES Integration Committee was formed to find the overlaps and intersections between different applications. Identification of the integration elements needed to connect individual application models has resulted in a "core" model called the Integrated Product Data Model (IPDM). This model is used to describe how the topical models can be merged into the complete PDES conceptual model.

The urgency to produce a PDES standard that is useful to the industrial community has forced the decision to define PDES as a collection of versions. Each new version enhances the product data definition available in the previous version. In addition, each new version will expand the scope of PDES to incorporate more life-cycle activities. As these versions are released, the techniques for representing the conceptual models may vary because of the new complexity and richness of the specified information. In addition, only the later versions will specify sufficient product data to allow database and knowledge base implementations to be efficiently built.

A conceptual model contains the fundamental objects and concepts managed by an enterprise. The conceptual model also depicts the relationships among the fundamental data objects of the enterprise. Fundamental data objects are combined to create useful collections of data which are subsets of the conceptual model, called external views. An "external view" consists of

user-specific data and the structural organization of that data. The procedures for creating the collections are unique recipes or instructions for manipulating the fundamental data. These procedures require management in their own right. They are not part of the conceptual model. The rules for deriving external views are user-specific and unique to each application.

Since the conceptual model includes all the important facts about an enterprise, it can be thought of as a detailed "database" containing vital constructs which can be extracted and viewed in various ways. Extracts can provide a mechanism to validate the content and intent of the conceptual model.

Once the first sharable topical product models were generated and integrated, the PDES group had to consider the following technical issue. How could the product model be represented in a totally unambiguous manner? The answer was to represent the information using a database design technique called "data modeling." The various PDES application subcommittees then implemented the specific topical data model in a variety of data modeling formats. This caused a problem at integration, as different data modeling techniques were used by different application subcommittees. As with all technologies, there are a range of tools, each of which is best for solving specific problems. Improved and extended data modeling techniques, as well as the tools to implement them, will continue to appear in the future. Because PDES will be an ever evolving standard, it is appropriate to allow the different topical data models to be defined using a variety of data modeling techniques.

To be able to tolerate and integrate multiple modeling techniques, a mechanism is needed for transferring specific data models between the competing data modeling techniques. An ideal candidate for this mechanism is a "data dictionary system" that can save the product data model in a neutral specification. Using a data dictionary system as this mechanism, it is then necessary to implement only one pair of translators for each data modeling technique. This allows for the translation of one data modeling representation into the neutral format, and the translation of the neutral format back into another data model representation. The data dictionary system also becomes an effective and efficient configuration manager for the development of the IPDM.

PRODUCT DATA MANAGEMENT

The IPDM, resulting from the integration of the merged topical models, abstractly defines the way in which the product data elements interrelate. In addition, the "physical level" defines the way the actual product data is represented, organized and stored (such as on a disk or in memory). [Figure 1] The PDES

community is currently defining levels of implementation for PDES. These levels define the "road map" for how product life-cycle activities (e.g. design, process planning, etc.) will interface to the PDES implementation.

This leads to the second major issue: the development of a mechanism that can manage the enterprise data and data semantics for use in PDES implementations. This information management capability can be supported by a data dictionary system that has adequate functionality. The data dictionary system must be able to interact with a variety of data storage techniques, such as relational databases, file systems, object oriented databases, etc. The data dictionary system must be able to describe the data structures (e.g. strings, numbers, dates, tables, geometric entities) that exist in the product information representation and be able to cross-reference the associations among these data structures. This PDES information must then be accessible to the life-cycle systems through a neutral language that may be dependent on the level of implementation but should not be dependent on the actual system implementation (i.e., the language of a given relational database management system (DBMS) or file management system).

APPROACH

The storage and management of all the components of PDES development information in one logical, standard, data dictionary system is the cornerstone for automation and reusability in the future. Such a data dictionary system is required to manage the numerous PDES topical and application models, model integration, the validation process and the necessary documentation.

The Information Resource Dictionary System (IRDS) standard being developed by the American National Standards Institute (ANSI) and the National Institute of Standards and Technology (NIST) can meet this need. The IRDS can be used to identify and control all of the "pieces" that make up PDES and to evaluate the effect of needed changes that will occur as the PDES standard emerges. With the use of the extensibility feature, the IRDS provides a stable platform for development and maintenance even when the underlying technology is changing. [Figure 2]

The IRDS can support system integration by merging development and maintenance tools into one environment. PDES development requires the use of data modeling tools, data dictionaries, DBMS, and, eventually, knowledge base systems to support all its functions. Commercial and public-domain products exist in all these areas. They can be easily obtained, but not easily interfaced. The IRDS can provide the mechanism by which these tools can be interfaced and replaced as new technologies emerge.

The IRDS can support the 3-schema architecture (i.e., the external view of the user, the logical conceptual model, and the physical or implementation view of the internal model). [Figure 3] Another way to visualize the three-schema architecture is as a 3-dimensional space, with the three axes representing use, processing and universality. Each of the three schemas--external, internal and conceptual -- can be represented as a point in this space. The major component of each of the schema points projects on a different axis: external projects on the use axis, internal projects on the processing axis, and conceptual projects on the universality axis.

This architecture permits the relationships between levels to be independently defined, permitting some changes to be made to the specifications at one level without affecting the specifications at the other levels. Major changes, such as expansion of scope, discovery of additional relationships, etc., will impact all levels. Therefore, it is important to know how each level is with the other through cross-referencing relationships. The IRDS is the only recognized information management standard in this area.

The IRDS provides a basic Functional Schema which directly supports much of the information that an organization needs to keep about implemented software systems. For example, the ability to describe the data elements that make up a record and how records are organized into a file is part of the IRDS Basic Functional Schema. Further, the IRDS provides a general schema extensibility mechanism for tailoring and adding types of information resources that need to be managed within an organization. Schema extensibility is provided since the IRDS does not intend to describe all of the types of resources that enterprises may need to manage with a data dictionary. What is provided by the standard is a schema with a minimum set of information resource types, to be used as an example, along with building blocks for extending the schema to meet each organization's needs. It is this extensibility feature which makes the use of IRDS so attractive.

What are the major categories of product data information resources that must be managed if the full potential of an information resource dictionary is to be realized for PDES? PDES information resources can be grouped into three categories:

1) implemented systems and data organizations,
2) conceptual models and business rules, and
3) data usage and external views of data.

If the data types provided by the IRDS Basic Functional Schema are examined, most of them fall within the first category of information resources. The IGES/PDES Organization has spent almost all its effort defining the second category of resource

types. Major efforts are still needed in the third category to define industry and activity specific views of PDES or application protocols.

To be a more complete and effective tool for the PDES community, the IRDS schema structures must be modeled with an Information Resource Dictionary (IRD) to store and access the conceptual IPDM. The schema of this IRD must be extended to capture and document the meaning of the entities, relationships and attributes which comprise the integrated conceptual model.

Once a neutral conceptual model is developed, the IRDS can be used to effect change control over existing applications and databases. Currently, IRDS provides facilities for recording, storing, and processing descriptions of data. It can create and store schemas for all types of data management systems. Thus, application programs will not need to incorporate the schemas into their code; programs can obtain the necessary information from the IRDS, resulting in a true data-driven system. The PDES dictionary can also serve as the access control point for all current models. The activities described below provide directions to pursue to support specific PDES needs. We are not attempting to address more general problems.

ACTIVITIES

1. Build a schema for a PDES Information Resource Dictionary, using the IRDS schema extensibility feature to support the storage and management of the diverse conceptual models built by the PDES committees.

   The extensibility feature of IRDS will be used to define a set of information resource types, called metatypes, which correspond to each of the fundamental constructs found within the conceptual modeling techniques used by PDES. This new schema definition will allow IRDS to support the storage and retrieval of conceptual models. Automatic dictionary loading and version-controlled updates must be added to the existing IRDS prototype to support management of the conceptual models.

2. Extend the PDES Information Resource Dictionary schema to support a full three-schema architecture, and populate the IRD with PDES information.

   Initially this repository will hold the conceptual models, supporting entity definitions, and scoping statements, as well as related, but unresolved, issues. The IRDS Basic Functional Schema supports only information describing the internal schema, specifically physical databases and files, computer hardware, and user profiles. Therefore, the PDES

IRD schema will be expanded to support a full three schema dictionary. When application subsets, testing criteria, test cases, and implementation guidelines are developed, the PDES dictionary can then be populated with relevant information. This will permit evaluation of the effects of changes and expansions in the PDES standard. These resources can then be brought into alignment with the standard.

3. Develop automated or assisted translation between diverse data models and represent these data models in the IRDS.

There are three types of data models being produced by PDES activities. PDES Version I will contain both EXPRESS and IDEF1X, two types of data models. In addition, some committees are formalizing their work in NIAM, a third type. A NIAM model must be translated into both IDEF1X and EXPRESS before it can be incorporated into the PDES standard. Equivalent concepts between these models must therefore be identified and formally represented to ensure that the different types are consistent. Translating these data models into the IRDS can provide PDES with a unified representation of this information, and permit consistency checking among the data models.

4. Interface the PDES Information Resource Dictionary to available software.

The IRDS provides for integration between data modeling tools, database and system design aids, and application development. As the repository for dictionary metadata describing functions, data, and objects that compose an application, the IRDS becomes the key integration tool for PDES application development. In addition, it provides the IRDS Export/Import Facility to control moving IRD schema and metadata definitions from one site to another. The IRDS Export/Import Facility is currently under development at NIST.

4.1 Utilize conceptual modeling tools.

These tools are used in the requirements analysis and system design phases. They provide quality controls in the definition of both data models and functional design. Most will also generate a prototype database schema in one or more relational data definition languages. Most also have an interchange form. This interchange form is the most likely method for interfacing these tools to the IRDS. No standardization efforts are active within ANSI to develop a standard conceptual modeling language that could be used for this purpose.

4.2 Support IRDS information interchange with DBMS.

DBMS provide a general purpose capability for storing, accessing, and managing actual instances of data. The Structured Query Language (SQL) standard and the Network Database Language (NDL) standard are expected to be the first of the DBMS related standards to be interfaced to the IRDS standard. Remote Data Access (RDA), an International Organization for Standardization (ISO) standards effort, is not yet mature enough for an interface to IRDS to be designed. RDA also supports less capability than a distributed PDES database implementation needs. However, ISO has done enough work in the distributed area to identify the minimum information requirements that a data dictionary/directory must manage to support this distributed aspect. The IRDS Service Interface, which is currently under review, is an addendum to the IRDS standard that will support the use of the IRDS in an active mode. The Services Interface is expected to be formally accepted as part of the IRDS standard in 1990-91.

5. Develop Relationships to Physical Design.

The PDES organization is not heavily concerned with how PDES is physically implemented because many of these issues fall under the domain of implementors. There are aspects of physical design, however, that must be managed to maintain consistent versions of PDES; PDES will produce an exchange format and testing suites which must conform to the conceptual models defined in the standard. Therefore the elements of the conceptual models must be associated with those of the exchange format and testing libraries. Further, there must be an ability to document the decisions made in the physical design of these modules and to detect changes required to keep these modules consistent with newer versions of PDES. These types of cross-referencing information can be captured and stored in the IRDS.

GLOSSARY

Application Model

A data model which addresses the information requirements for a specific industry or vital business objective such as electrical design or structural analysis.

Conceptual Model

An abstraction of the real world that conveys the concepts, meaning and semantics of information for an organization. It forms the basis for a dialogue between systems and users and is based on a common understanding of the information it represents.

Data Attributes

Properties of product data which describe the data objects.

Data Dictionary

A repository for data definitions, system documentation, data representations, and requirements descriptions of information managed within the automated or manual systems of an organization. This resource is then available over the life-cycle of developing and existing systems.

Enterprise

May be a corporation, a unit or division of a corporation, government unit, or group of cooperating organizations, etc., which is the source or owner of information.

External View

That set of information which is sufficient to support the performance of a particular function or business objective.

Fundamental Constructs

Defines the basic constructs used to create the data model. Each data model technique will have a set of primitive elements that are used to formally describe an actual data model.

Heterogeneity

Use of dissimilar computer hardware and software in support of a common objective.

Implementation Model

A design of the data organization for a system. For database systems this would be a database schema in the definition language of the database management system selected to implement the system. For applications, this would be the data structures in the computer language used to write the application and for object oriented systems, this would be the object class definitions.

Integration

The process of merging together independently developed models into a cohesive and consistent model which reflects a common understanding of information resources used within an enterprise.

IRD Data Layer

The layer of the information resource dictionary that manages the actual descriptions of information resources.

IRD-IRD Interface Facility

A method of exchanging information resource dictionaries to additional sites which may have processing responsibilities.

IRD Schema Description Layer

Provides the basic framework on which to build the types of information resources to be managed within an information resource dictionary.

IRD Schema Layer

Defines the types of information resources to be managed within an information resource dictionary; these are called metatypes.

IRDS

The Information Resource Dictionary Standard is a draft proposed ISI and FIPS data dictionary standard.

Knowledge Base

A system which is capable of persistent data management and can actively enforce the business rules defined against the data. A knowledge base is capable of evaluating requested functions and performing constraint checking on the data. -

Level I Implementation

A passive file interchange implementation of PDES.

Level II Implementation

An active file interchange implementation of PDES.

Level III Implementation

A database implementation of PDES.

Level IV Implementation

A knowledge base implementation of PDES.

Life-Cycle

The distinct phases into which every system may be divided such as requirements, design, implementation, production, and maintenance. Each phase may require different support from the data dictionary which is used to administrate it.

NDL

The Network Database Language is the ANSI standard for data definition and access for network databases.

Physical Design

The process of evaluating an implementation model or design and factoring in performance characteristics and data access to optimize the design.

PDES

Product Data Exchange Specification is a developing standard which will provide for the unambiguous interchange of life cycle product data from concept, to engineering design, to manufacture, and to support.

RDA

The Remote Data Access protocol is an ISO standards activity which is developing a standard for distributed system access.

SQL

The Structured Query Language is the ANSI standard data definition and access for relational databases.

Topical Model

A data model which incorporates the requirements of many users into a data model of limited scope. The scope defines the topic of the data model (e.g. geometry data model).

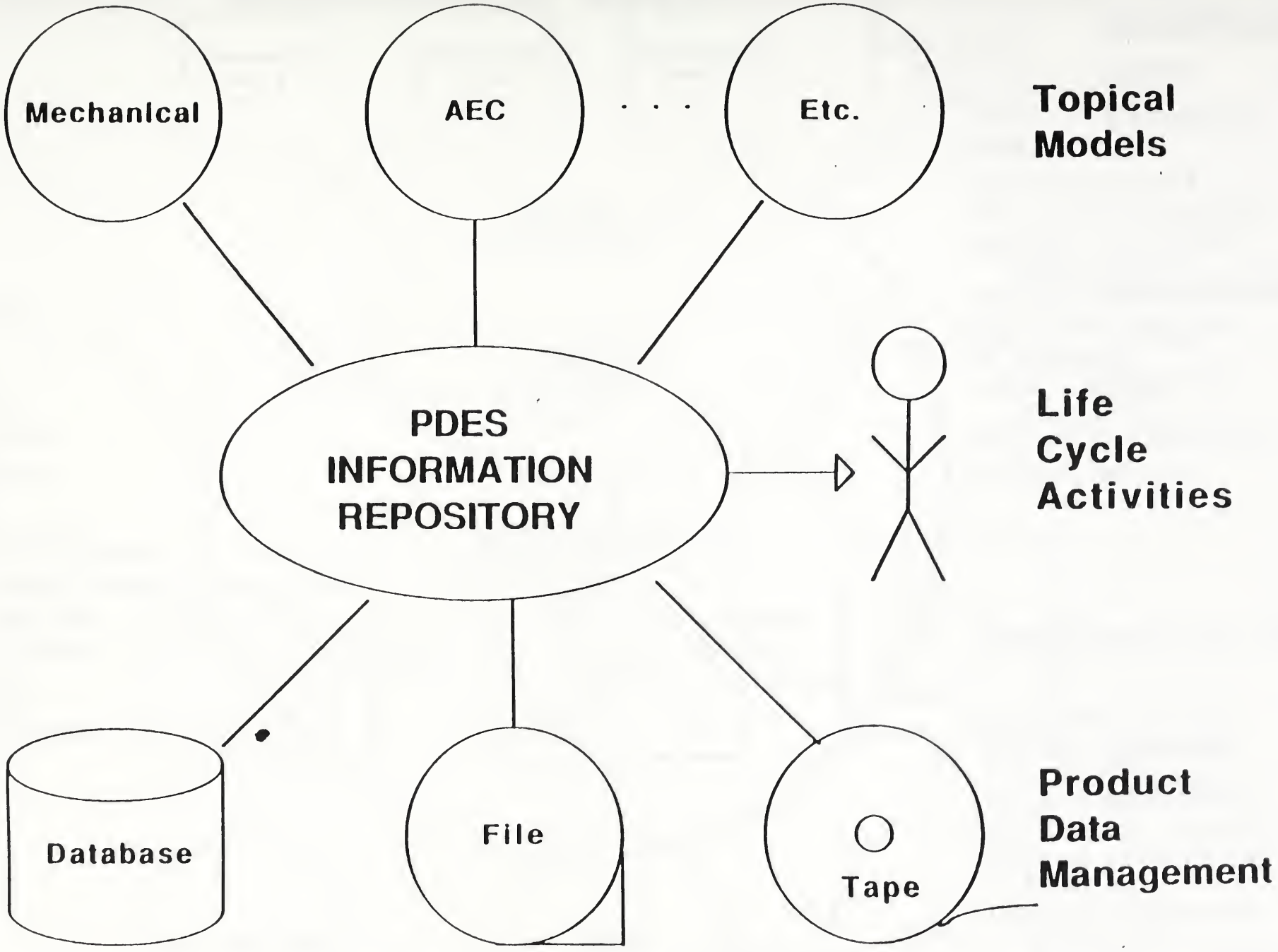

Mechanical
AEC
Etc.
Topical Models
PDES INFORMATION REPOSITORY
Life Cycle Activities
Database
File
Tape
Product Data Management

Figure 1

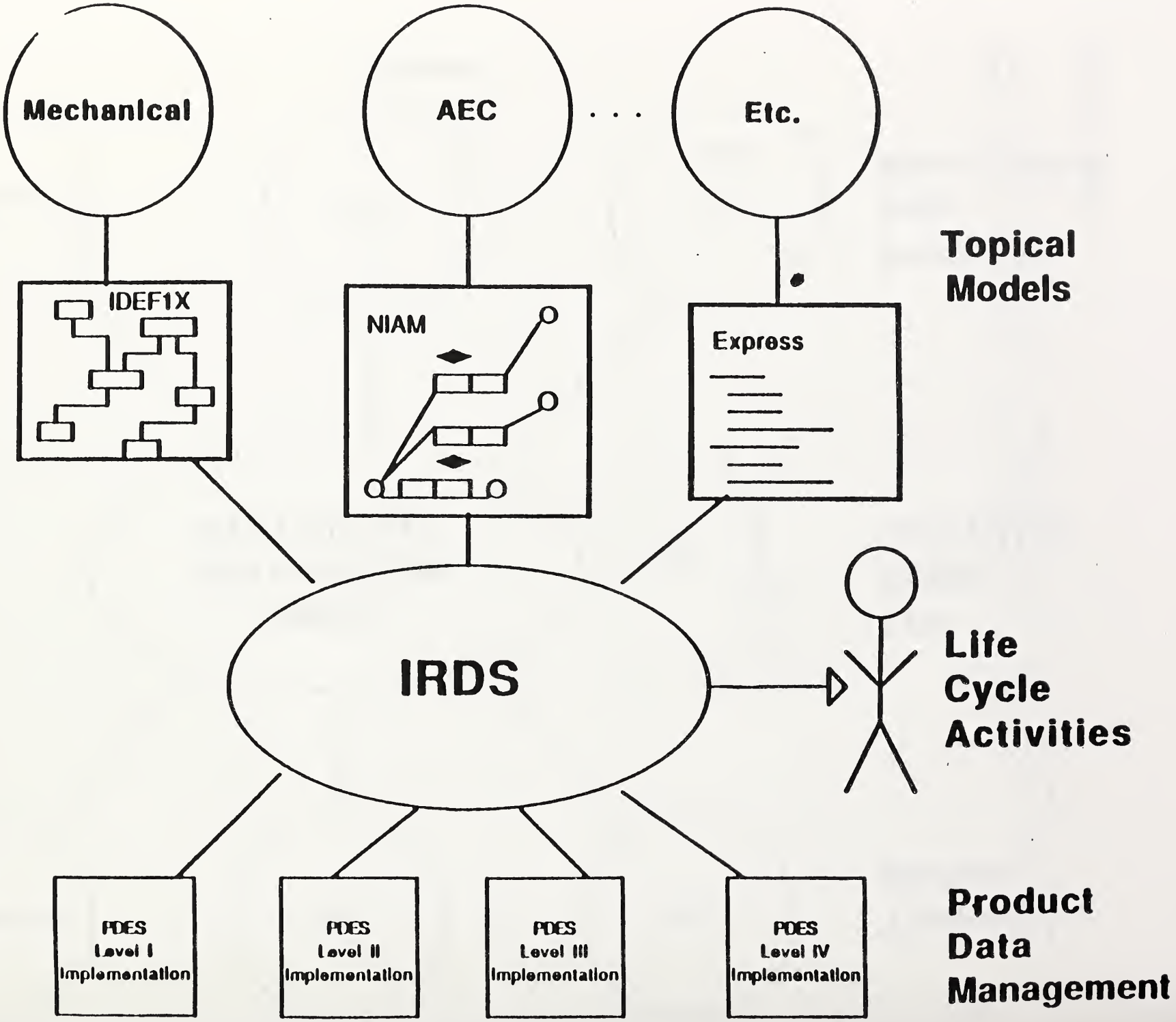

Mechanical
AEC
Etc.
Topical Models
IDEF1X
NIAM
Express
IRDS
Life Cycle Activities
PDES Level I Implementation
PDES Level II Implementation
PDES Level III Implementation
PDES Level IV Implementation
Product Data Management

Figure 2

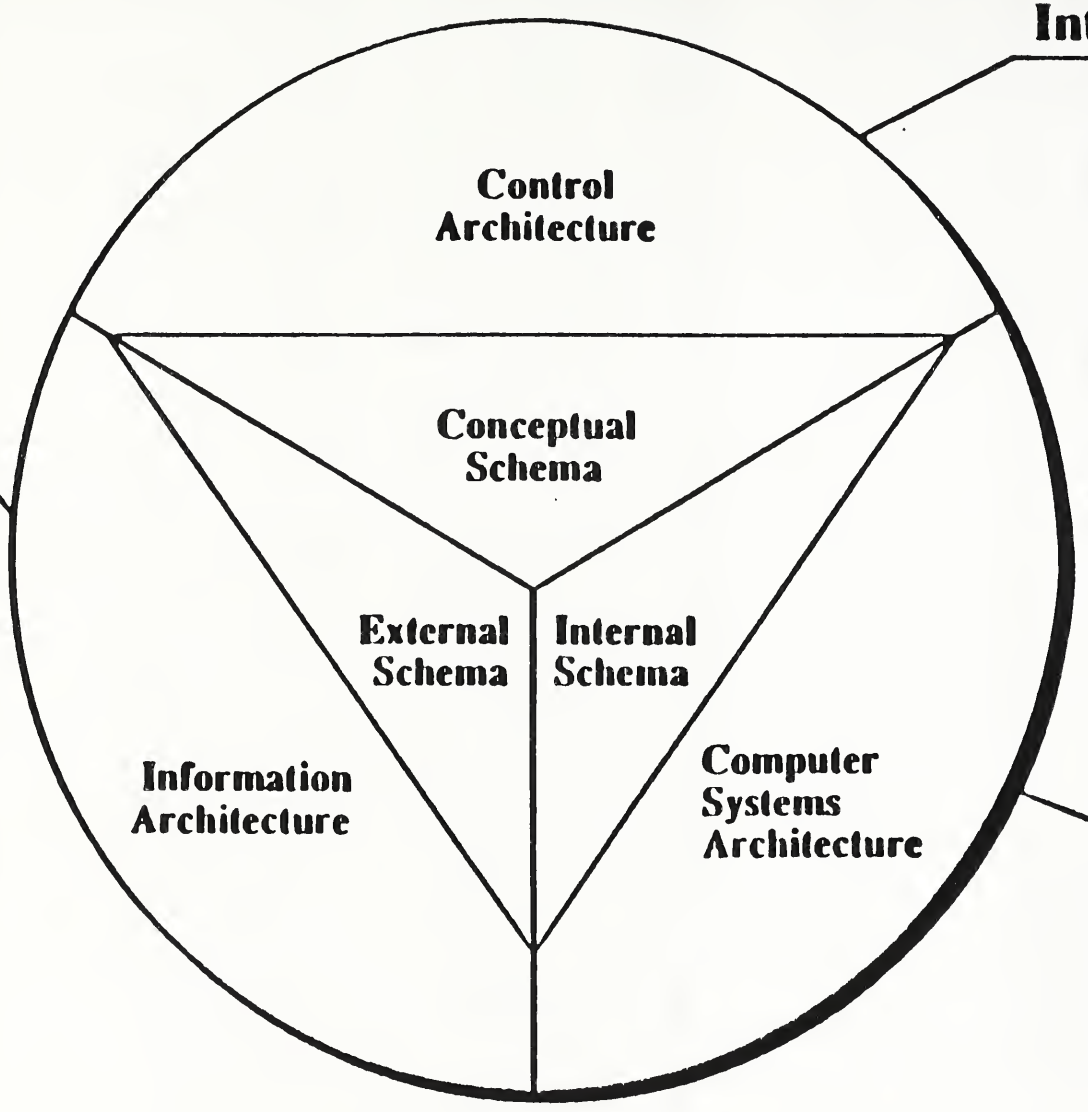
ENTERPRISE STRUCTURE

Integrated View

- Business Rules
- Conceptual Model
- Life Cycle Management
- Systems Development Methodologies
- Data Administration
- Information Planning Processes
- Project Management Procedures
- Programming Standards
- Vendor Contracts

User View

- Requirements Definitions
- Project Resources
- Standard Reports
- Applications
- Business Objectives
- Functional Areas Affected
- Automation Requirements
- Anticipated Benefits
- Management Support
- Project Scopes
- Activity Models
- Project Data Models



Data Processing View

- Computer Hardware
- Computer Security
- User Profiles
- Systems Software
- Applications Programs
- Physical Databases & Files
- Database Management Software
- Communications Software

Components of the Three Architectures

NIST-114A
(REV. 3-89)

U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

BIBLIOGRAPHIC DATA SHEET

1. PUBLICATION OR REPORT NUMBER
NISTIR 4315

2. PERFORMING ORGANIZATION REPORT NUMBER

3. PUBLICATION DATE
MARCH 1991

4. TITLE AND SUBTITLE

A Collection of Technical Studies Completed for the Computer-Aided Acquistion and Logistic Support (CALS) Program Fiscal Year 1988 Volume 1 of 3, Text, Security and Data Management

5. AUTHOR(S)

Roy S. Morgan, Editor

6. PERFORMING ORGANIZATION (IF JOINT OR OTHER THAN NIST, SEE INSTRUCTIONS)

U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
GAITHERSBURG, MD 20899

7. CONTRACT/GRANT NUMBER

8. TYPE OF REPORT AND PERIOD COVERED
NISTIR 10/87 - 9/88

9. SPONSORING ORGANIZATION NAME AND COMPLETE ADDRESS (STREET, CITY, STATE, ZIP)

Office of the Secretary of Defense
Production and Logistics/Systems/CALS
Room 3B322, Pentagon
Washington, D.C. 20301-8000

10. SUPPLEMENTARY NOTES

[ ] DOCUMENT DESCRIBES A COMPUTER PROGRAM; SF-185, FIPS SOFTWARE SUMMARY, IS ATTACHED.

11. ABSTRACT (A 200-WORD OR LESS FACTUAL SUMMARY OF MOST SIGNIFICANT INFORMATION. IF DOCUMENT INCLUDES A SIGNIFICANT BIBLIOGRAPHY OR LITERATURE SURVEY, MENTION IT HERE.)

Computer-aided Acquistion and Logistic Support (CALS) Program is a DoD and Industry strategy to transition from paper-intensive acquisition and logistic processes to a highly automated and integrated mode of operation for the weapon systems of the 1990s. These volumes document the accomplishments of the National Institute of Standards and Technology to advance the development of technology and standards in support of CALS. These reports are divided into three volumes: 1, Test, Security, and Data Management; 2, Graphics, CGM MIL-SPEC; and 3, Graphics, CGM MIL-SPEC; and 3, Graphics, CGM Registration.

Volume 1. Text, Security and Data Management: Work on text and graphics standards in the CALS publishing environment is described, including technology assessments, application guidance, conformance test plans and a draft Federal Information Processing Standard (FIPS) for ODA/ODIF. Additionally, a technology assessment and proposed conformance testing strategy for page description management tools is presented with a discussion of computer security issues. The use of the Information Resource Dictionary System, (IRDS, ANSI Standard X3. 138-1988) is proposed as an integration and configuration management mechanism for the Product Data Exchange Specification (PDES).

12. KEY WORDS (6 TO 12 ENTRIES; ALPHABETICAL ORDER; CAPITALIZE ONLY PROPER NAMES; AND SEPARATE KEY WORDS BY SEMICOLONS)

conformance testing; data management; ODA; ODIF; PDES: publishing; security; text

13. AVAILABILITY

[X] UNLIMITED

[ ] FOR OFFICIAL DISTRIBUTION. DO NOT RELEASE TO NATIONAL TECHNICAL INFORMATION SERVICE (NTIS).

[ ] ORDER FROM SUPERINTENDENT OF DOCUMENTS, U.S. GOVERNMENT PRINTING OFFICE, WASHINGTON, DC 20402.

[X] ORDER FROM NATIONAL TECHNICAL INFORMATION SERVICE (NTIS), SPRINGFIELD, VA 22161.

14. NUMBER OF PRINTED PAGES
253

15. PRICE
A12

ELECTRONIC FORM