DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

This report has been reproduced directly from the best available copy.

Available to DOE and DOE contractors from the Office of Scientific and Technical Information, P.O. Box 62, Oak Ridge, TN 37831; prices available from (615) 576-8401, FTS 626-8401.

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table of Contents</td>
<td></td>
</tr>
<tr>
<td><strong>Preface</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Introduction</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Principles</strong></td>
<td></td>
</tr>
<tr>
<td>Network Topology</td>
<td>NT-1</td>
</tr>
<tr>
<td>Network Protocols</td>
<td>NP-1</td>
</tr>
<tr>
<td>Network Administration</td>
<td>NA-1</td>
</tr>
<tr>
<td>General Platforms</td>
<td>GP-1</td>
</tr>
<tr>
<td>File Servers</td>
<td>FS-1</td>
</tr>
<tr>
<td>Workstations</td>
<td>WS-1</td>
</tr>
<tr>
<td>Information Servers</td>
<td>IS-1</td>
</tr>
<tr>
<td>Peripherals</td>
<td>PP-1</td>
</tr>
<tr>
<td>Electronic Documents</td>
<td>ED-1</td>
</tr>
<tr>
<td>Desktop Office Products</td>
<td>DP-1</td>
</tr>
<tr>
<td>Document Management</td>
<td>DM-1</td>
</tr>
<tr>
<td>Electronic Routing</td>
<td>ER-1</td>
</tr>
<tr>
<td>Electronic Mail</td>
<td>EM-1</td>
</tr>
<tr>
<td>Directory Services</td>
<td>DS-1</td>
</tr>
<tr>
<td><strong>Figures</strong></td>
<td></td>
</tr>
<tr>
<td>Network Schematic</td>
<td>NS-1</td>
</tr>
<tr>
<td>File Server Connections</td>
<td>FC-1</td>
</tr>
<tr>
<td><strong>Scenarios</strong></td>
<td></td>
</tr>
<tr>
<td>File Server and Workstation Environment</td>
<td>WE-1</td>
</tr>
<tr>
<td>Peripheral Use</td>
<td>PU-1</td>
</tr>
<tr>
<td>Applications Platform</td>
<td>AP-1</td>
</tr>
<tr>
<td>Network Installation</td>
<td>NI-1</td>
</tr>
<tr>
<td>Workgroup and Managed Documents</td>
<td>WD-1</td>
</tr>
<tr>
<td>Document Review</td>
<td>DR-1</td>
</tr>
<tr>
<td>Document Index Searching</td>
<td>DI-1</td>
</tr>
</tbody>
</table>
Preface

A computing infrastructure design architecture is a framework for making decisions about the implementation of information systems and their supporting infrastructure. This document presents the desired Savannah River Site Computing Infrastructure Design Architecture and was developed jointly by the Advanced Technology and Architecture (ATA) Section of the Information Resource Management (IRM) Department with the support and approval of the site Computing Architecture and Standards Team (CAST). CAST has representation from all site divisions, and additional representatives from manufacturing computing (Process Digital Equipment Committee), engineering and scientific computing (Engineering/Scientific Computing Committee), and management information systems (Information Resource Management).

Any comments or questions concerning the content of the document or the site computing infrastructure design architecture should be addressed to ATA or any member of CAST.

The following are the current members of CAST and ATA personnel who participated in developing this document:

R. R. Beckmeyer
L. T. Bertsch
A. E. Blanchard
G. L. Bonham
W. H. Brotherton
R. R. Butterworth
R. L. Cavaliere
J. M. Cloninger
G. L. Custodi
D. W. Eckert
W. C. Foster
D. E. Gordon
A. J. Johnson
J. L. Kirk
T. D. Kohli
B. F. Meadows
J. M. O'Leary
C. M. Schaumann
E. E. Smith
C. F. Stanland
G. P. Thompson
T. T. Thompson
F. D. Knight
Introduction

Purpose

While the SRS Computing Architecture (Reference 1) outlines the overall vision for site computing, it does not address the many high-level design decisions needed to implement that architecture. Without additional guidance, site organizations could select from the many available implementation options, and as a result, they could implement solutions or specify products that are not compatible across the site and thus make the architecture goal of sitewide interoperability impossible. In an effort to reduce the occurrences of such situations, design architectures are being developed to fill the gap between the overall vision of the SRS Computing Architecture and the detailed design and product decisions which implement the architecture.

This document enumerates the principles, scenarios, and strategies which capture the essence of architectural design decisions which have been made for the computing infrastructure. Its objective is to guide the designers of infrastructure components to reduce the number of design decisions which must be made, to document and justify decisions which have already been made, and to promote consistent, interoperable, cost-effective implementations. Designers and implementers should consult the Design Architecture throughout the life of a project to ensure compliance and to guarantee that conceptual integrity is maintained.

Changing needs of the site, as well as emerging technologies, will cause future implementation changes. This document attempts to provide guidance for an approximately three-year window to the future, and will be updated periodically. In some areas, such as multimedia computing, implementation issues are still being identified. These areas will be further addressed in updated versions of this document.

Scope

As stated in the SRS Computing Architecture, the future vision of computing at the Savannah River Site is "standards-based, data-driven, and workstation-oriented, with larger systems being utilized for the delivery of needed information to users in a client-server relationship." Just as the implementation of host-based applications required a robust, secure, and consistent platform, the delivery of client-server applications also requires a supporting infrastructure.

The familiar house analogy can help us understand the concept of computing infrastructure. In a house, the infrastructure consists of the wiring, plumbing, foundation, heating, air conditioning, etc. While not a primary activity within the house, it is nevertheless a critical support function for other activities. Reading, cooking, eating, cleaning, sleeping, etc. all depend upon components of the infrastructure.
The infrastructure is so pervasive, however, that it is often overlooked. For example, we tend to take for granted the fact that air conditioning is present in every room until we walk into an uncooled garage in the summer. The distinction as to where infrastructure ends and its application begins is sometimes cloudy, as well. For example, is a built-in oven part of the infrastructure? What about a refrigerator? Finally, while the infrastructure (e.g., wires, pipes, and ducts) is largely hidden, there are definite interfaces (e.g., outlets, faucets, and vents) with which we interact so that it is not totally transparent.

The definition of computing infrastructure used within this document includes site network components, protocols, topology, administrative practices workstations, peripherals, various server systems (such as file and information servers), document manipulation, interpersonal messaging, groupware, etc.

The Computing Architecture specifies an integrated environment based upon standards and the interoperability of networked computers. A robust communications infrastructure must be established and maintained to leverage the true power of workstations through client-server computing and to support rapid access to large amounts of data. In an environment in which all workstations and servers are network-attached, this means that maintaining adequate bandwidth must be as high a priority as availability. This requirement therefore manifests itself in the network topology, the protocol selection, and the administrative practices.

Historically, most applications executed on large system platforms which hosted users by way of terminals or workstations emulating terminals. In the future, large system platforms will function primarily as information servers, providing data and computation services for client applications executing at the workstation level. Through standardization, workstations and file servers will also become an integral part of the platform infrastructure to provide the workstation connectivity, manageability, and usability features which all applications will require.

Office computing includes those productivity tools which are provided on a site-wide basis and will include products such as electronic mail, electronic routing, etc. It also includes electronic documents, the software products which manipulate them, the formats in which they are stored, and a mechanism for sharing them. Office computing products are currently in both a top-down transition (i.e., from host-terminal to client-server implementations) and a bottom-up transition (i.e., from standalone workstations to LANs). For this reason, it is still too early to make definitive architectural decisions for many product categories.

By its nature, an infrastructure must attempt to accommodate diverse needs, requiring some compromises. Although the focus of this release of this document is on business and office computing, all designs must be consistent with the needs of engineering, scientific, and process-control computing. Future releases of this document will be required to address these interactions.
As in the house analogy, the distinction between infrastructure and applications can sometimes blur, especially in areas such as office computing where there is a high degree of human-machine interaction. In this document, the computing infrastructure is defined as those components which are fundamental to the overall computing environment, which enable sitewide interoperability, and which are pervasive.

This document, like the *SRS Computing Architecture*, is focused on areas most applicable to traditional computer information systems and does not attempt to address the unique requirements of scientific and engineering computing, process computing, or classified computing applications. However, the architectural principles and directions put forth in this document may be applied to *any* area of computing, provided they do not conflict with other site requirements.
References


### Principles

This section specifies design principles in the following areas:

<table>
<thead>
<tr>
<th>Area</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Topology</td>
<td>Describes the physical components of the network.</td>
</tr>
<tr>
<td>Network Protocols</td>
<td>Specifies protocol constraints and routing philosophy.</td>
</tr>
<tr>
<td>Network Administration</td>
<td>Outlines network operation and management principles.</td>
</tr>
<tr>
<td>General</td>
<td>Lists principles which apply to all platforms.</td>
</tr>
<tr>
<td>File Servers</td>
<td>Describes file server configurations and deployment.</td>
</tr>
<tr>
<td>Workstations</td>
<td>Specifies standard workstation configurations and rules for integrating workstations into the network environment.</td>
</tr>
<tr>
<td>Information Servers</td>
<td>Lists principles for servers other than file servers.</td>
</tr>
<tr>
<td>Peripherals</td>
<td>Provides guidance on implementation of input/output devices.</td>
</tr>
<tr>
<td>Electronic Documents</td>
<td>Lists storage and access principles for documents.</td>
</tr>
<tr>
<td>Desktop Office Products</td>
<td>Specifies requirements for commercial workstation applications.</td>
</tr>
<tr>
<td>Document Management</td>
<td>Addresses the generation, revision, storage, and distribution of formal documents.</td>
</tr>
<tr>
<td>Electronic Routing</td>
<td>Lists principles for a sitewide document routing utility.</td>
</tr>
<tr>
<td>Electronic Mail</td>
<td>Specifies requirements for the electronic messaging environment.</td>
</tr>
<tr>
<td>Directory Services</td>
<td>Lists addressing and directory principles.</td>
</tr>
</tbody>
</table>
Network Topology

Description

Network topology refers to the implementation of the physical components of the network, such as bridges, routers, cabling, etc., which are required for the interconnection of workstations, printers, and servers. Many of the rules for network topology are inherent in the technology (e.g., the “two repeater rule” for Ethernet networks) and are not repeated here. SRS-specific conventions are necessary, however, to ensure that our network is configured in a robust, supportable, and scalable fashion.

The network topology must be flexible enough to allow for increasing bandwidth where necessary to support future applications while being cost-effective to install in the current environment.

Note: The term Ethernet in this document refers to either Ethernet version 2 or IEEE 802.3, unless explicitly stated.

Principles

NT.1 Network traffic will be minimized.

Because of the large number of workstations that will ultimately be supported by the site network, implementations should be designed to minimize network traffic wherever cost effective and consistent with other design objectives.

NT.2 The site network will consist of multiple sub-networks interconnected to form a single logical network.

Interconnection of site networks is essential to providing an integrated computing environment.

NT.3 A maximum of 200 user devices will be supported per sub-network.

Network addressing plans can only allow 250 IP devices per sub-network. Some of these addresses must be reserved for routers and special services, so the design goals do not exceed 200 devices per sub-network for any protocol. More importantly, 200 devices (printers, workstations, and servers combined) has been selected as a current maximum based upon expected network traffic.

NT.4 Sub-networks will have boundaries consistent with geographic boundaries.

If two sub-networks exist in a two-story building, each floor will be a sub-network exclusively. A single-story building with two sub-networks will be
divided evenly along corridors. Several trailers may comprise a sub-network, but a trailer will not contain two sub-networks.

This plan simplifies address assignment and minimizes wiring problems. In some situations, a special network (for high-traffic devices or those dealing in special information) might coexist. Appropriate labeling will be required to avoid confusion.

NT.5 Workstations and servers will have direct (Ethernet or FDDI) network connections.

Workstations will be migrated from serial (terminal server or 3270) connections to direct network connections. Ethernet will be the primary connection mechanism for workstations as well as servers, although FDDI will be used where very high throughput is required.

NT.6 Universal wiring will support both Ethernet and FDDI connections.

Universal wiring, terminating in communications closets, will be installed for every knowledge worker location. Facilities with non-standard wiring will be re-wired. Although Ethernet by way of 10BaseT is currently the site standard for workstation connections, the site standard for universal wiring has been changed to include one connection supported by data grade twisted pairs (DTP). This wiring will provide the flexibility to eventually support FDDI links to desktop workstations.

NT.7 Token Ring use will be restricted to support of the IBM Central Computing Facility.

The local area networking standard is Ethernet. There will be an "Apex" ring at the CCF and one or more minimal remote token rings to support special CCF communications requirements. The rings will interconnect via source route bridging on the site network.

NT.8 Fiber optic cabling will be used to interconnect buildings.

Fiber is preferred to coaxial cable for interconnections between buildings since it not only provides electrical isolation but also facilitates eventual migration to FDDI. Buildings will be interconnected using single mode (8-10/125 micron) and multimode (62.5/125 micron) fibers. Trailers will be interconnected using multimode (62.5/125 micron) fibers.

NT.9 FDDI will be the standard for intra-area network trunks.

As the traffic on individual Ethernet segments increases, the bandwidth available on the trunks interconnecting those segments must increase accordingly. Additionally, high performance systems will be implementing interfaces capable of transmitting at speeds significantly faster than that supported by Ethernet.
NT.10 Inter-area circuits will support at least T3 speeds.

Existing T1 (1.5Mbps) circuits will eventually be overwhelmed by the network traffic between areas, even in a routed environment. Inter-area circuits will be migrated to T3 (45Mbps) or faster speeds.

NT.11 Use of the site broadband for data communications will be phased out; in the interim, it will be used only where there is no alternative.

The broadband is subject to a number of factors that make it less reliable for data communications than dedicated circuits.
Network Protocols

Description

To maintain a flexible and scalable network configuration, network traffic on one segment must be isolated as much as possible from other segments. This is most effectively done using a routed network and by supporting the management of a small number of routable protocols.

Principles

NP.1 Ethernet version 2 will be replaced by 802.3.

The site will migrate away from the current Ethernet version 2 packet encapsulation in favor of that defined by the IEEE 802.3 standard. This migration will likely take several years.

NP.2 Network traffic between sub-networks will be routed.

Routing will isolate most traffic, such as application downloading, to a single sub-network. This approach will minimize bandwidth utilization by isolating extraneous traffic.

NP.3 Non-routable protocols will be phased out.

Non-routable protocols will allow broadcast traffic to propagate to all network segments and contribute to the overall “background noise” on the network. These protocols will be phased out to facilitate migration to routed sub-networks. Site standard protocols are defined in Reference 5.

NP.4 Network routing will be performed by dedicated routers.

Since they are specifically designed for that purpose, dedicated routers are more efficient than servers or workstations.

NP.5 TCP/IP will be the preferred protocol for interconnectivity until commercial OSI implementations are mature and available.

Although compliance with the full OSI protocol suite will ultimately be required by GOSIP, products adhering to the specifications are generally immature or unavailable. The Computing Architecture specifies that TCP/IP will be used as a transition to OSI and that TCP/IP support will be implemented on all SRS platforms as it becomes available.

NP.6 The number of protocols supported on a workstation will be minimized.

Current implementations for the majority of workstations (IBM and Apple) cannot support a single protocol for all services. There is a strong effort to pressure vendors to provide TCP/IP support for file and print services.
In general, workstations currently will need to support at most two protocol stacks—TCP/IP and the protocol necessary for file and print service—order to adequately meet user requirements. The file/print protocols are workstation-dependent and include IPX and Appletalk.
Network Administration

Description

A large complex network, even if it's well designed, will not be robust unless it is properly managed and maintained. Network administration includes all those activities normally associated with the administration of large systems: configuration control, usage monitoring, capacity planning, hardware maintenance, security management, disaster recovery planning, etc.

Principles

NA.1 Process-control (data highways) and classified networks will remain disconnected from the site network. All other networks are part of the site infrastructure.

Unconnected networks should be avoided as they impede the flow of information among workers. Security concerns, however, will dictate the need for some specialized, unconnected networks.

NA.2 The site network will be centrally administered.

Central administration is necessary to maintain conceptual integrity and supportability of the network. This includes network design, implementation, change control, maintenance address management, and security administration.

NA.3 Network administration will strive for 7-day, 24-hour availability.

In an environment of networked workstations and client-server applications, continuous network availability is critical. Continuous, proactive monitoring and management are essential to maintaining a robust implementation. Some network applications may also require redundant hardware installations to maintain the required level of service.

NA.4 The network will be configured so as to be approved for transmission of UCNI and sensitive unclassified data.

To facilitate data sharing and interoperability, information exchange between unclassified systems should not be restricted by the network.

NA.5 Secure gateways will be used to control access to non-SRS networks.

Information exchange with non-SRS networks, such as the Internet, will be done through secure gateways which control incoming and outbound connections.

NA.6 Formal disaster recovery plans will be maintained for the network.
A robust network is essential to a successful computing environment, and disaster recovery plans are a key component in maintaining high availability. Formal planning ensures that appropriate facilities, training, and procedures are in place to provide rapid response in the event of a failure.

Network equipment will support remote management via industry standard mechanisms. Intelligent network devices (such as routers, bridges, and wiring hubs) will support remote management through protocols such as TCP/IP's Simple Network Management Protocol (SNMP). This allows a network manager to monitor and configure the network by querying information about the state of network devices and by changing the operating characteristics of the device, respectively.
General Platforms

Description

The following principles apply to all platforms, including workstations, file servers, and information servers.

Principles

GP.1 Platform components will be modular to facilitate evolution and minimize product-specific dependencies.

The technologies associated with desktop integration, including workstation and server hardware, graphical user interfaces, network operating systems, and groupware products, are evolving rapidly. Flexibility to respond rapidly to these changing technologies and the dynamic marketplace which results is essential to desktop integration. The required flexibility can be achieved only through modularity of components.

GP.2 System software will be maintained at vendor-supported versions.

In some cases, such as in dedicated process control systems or embedded systems, upgrades may be deferred or precluded due to configuration control requirements. Business and office support systems should, however, be maintained at version levels supported by the vendors. Unsupported versions of an operating system put the site in a higher risk and potentially higher support cost situation. Upgrades will be coordinated with training and support to reduce the impact on users.

GP.3 Development / testing environments will be provided for all platforms.

For each production platform, a non-production environment will be provided for the development and testing of new system software and hardware. These facilities are necessary to isolate testing associated with system upgrades and pilot projects from the production environment. The development / testing environment may take the form of a separate system or an isolated environment on an existing system, whichever is more cost-effective.

GP.4 All servers will be configured so as to be approved for storage and processing of UCNI and sensitive unclassified data.

To facilitate data sharing and interoperability, information exchange should not be restricted due to differences in security approval of unclassified systems. All large system installations will provide equivalent levels of protection.
GP.5 The procurement of obsolete hardware will be avoided.

In some cases, such as in dedicated process control systems or embedded systems, obsolete hardware may be required as an exact replacement due to configuration control requirement. Business and office support systems should, however, use hardware which will be cost-effective to install, integrate, and maintain.

GP.6 All servers will be covered by formal disaster recovery plans.

Robust platforms are essential to a successful computing environment, and disaster recovery plans are a key component in maintaining high availability. Formal planning ensures that appropriate facilities, training, and procedures are in place to provide rapid response in the event of a failure. The plan should provide guidance on the impact of loss of service and balance recovery actions to appropriate costs.

GP.7 Backups will be the responsibility of the storage service provider.

The organization operating the storage space is responsible for ensuring that the data stored on it is properly backed up. Backup of infrastructure servers will be centrally coordinated. Information servers will be backed up by the provider of that service. Workstation storage should be dataless or be backed up by the custodian of the workstation.
File Servers

Description

File servers provide the basic mechanism for the management of application software and workstation configurations. They also provide a robust and universally accessible platform for the storage of user document files. Because these servers will be so pervasive, management will be accomplished by specifying standard server configurations and by centralizing administration. (Note: This section applies only to business and office file servers which are provided as part of the site computing infrastructure. It does not apply to special application or restricted-use servers).

Principles

FS.1 File servers will be accessible from all supported workstation types in native mode.

For example, to a DOS user, the file spaces will appear as standard drive letters with subdirectories, while to a Mac user, the spaces would appear as AppleShare volumes with folders.

FS.2 File server configurations will be standardized.

A limited number of standard file server configurations will be defined to ensure consistency and manageability in a large-scale implementation. It is not cost-effective to attempt to manage unique file server configurations for each workgroup on site.

FS.3 File servers will be centrally administered.

Central administration of file servers is necessary to ensure consistency.

FS.4 File servers will contain logically separate data and system spaces.

System space will contain network operating system, file serving, print serving, and application software. The system space will be logically separate from data space to simplify upgrades and disaster recovery.

FS.5 File servers of a given type will have identical system space contents.

Uniqueness of servers will be minimized whenever possible. Except for configuration files, all system files will be identical. This standardization is a key design element which is required to facilitate central administration and disaster recovery.

FS.6 At least one file server will be installed per sub-network. This will be referred to as a "territorial" file server.
A file server will be installed on each sub-network to support the
workstations connected to that sub-network and to provide file space for
the users normally assigned to those workstations.

FS.7 Territorial file servers will be used to provide access to site standard
commercial software and standard site-developed applications.

Standard applications will be maintained in an execute-only file space on
territorial servers. Maintaining standard applications on the file servers is
more cost-effective than installing them on workstation local storage,
since it allows for fast, convenient upgrades and ensures that the
software being used is both current and legal.

FS.8 Territorial file servers will provide print services and print server support.

Shared print services across the network will provide users with
transparent access to any desired printer for which they are authorized.
The workstation or network will adjust to the capabilities of the selected
printer automatically.

FS.9 Territorial file servers will provide private data space for users within their
sub-network.

Each user will have a private space on a file server which is
automatically available upon login. Although the actual location of this
space is transparent to the user, it will typically be on a file server within
the same sub-network as the user's normal office location.

FS.10 User-specific configuration files will be stored on a user's assigned
territorial file server to promote workstation independence.

Upon entering the network, those characteristics defined as personal will
be used to recreate the desktop conditions such as color, style, and user
preferences that make each user's configuration unique. This "portable
desktop" provides users the flexibility to work at any workstation of the
same type as their normally assigned workstation while still having their
personal preferences. Maintenance of this information on the network will
be automatic and transparent to the user.

FS.11 File servers will be used to provide shared data space for workgroups.

Each workgroup will be assigned to a file server where a workgroup
shareable file space will be created. A file server may support multiple
workgroups. The members of a workgroup will have individual access to
the appropriate workgroup file space.

FS.12 Users may connect to multiple workgroup spaces.

Depending upon their job functions and file exchange requirements,
users may dynamically request connection to a file server, or they may
specify that the connection occur automatically upon login.
FS.13 The contents of the workgroup space will be the responsibility of the workgroup.

Although backup of the data space will be centrally administered, it will be the responsibility of the workgroup to ensure the correctness of the data. In the event that applications, either commercial or locally-produced, are placed in workgroup spaces, proper licensing and upgrading of those applications will be a workgroup responsibility.

FS.14 Workgroup administrators will be provided mechanisms to control access to their workgroup space.

One or more administrators will be designated within each workgroup to control access to files. This practice will allow the designation of read-only or controlled access on a per-user basis.
Workstations

Description

Workstations will be increasingly treated as an enterprise asset rather than as "personal" systems. Consistency of the workstation environment will be critical to supporting client-server computing, and will be achieved through standard configurations and automatic updates. Graphical user interfaces and communications mechanisms will be provided as well.

Principles

WS.1 Workstations are site resources.

A workstation is not owned by an individual but is a site resource much like a telephone. It may be redistributed to maximize its use or it may be shared by multiple users.

WS.2 Multiple standard workstations will be supported.

Site computing standards (Reference 5) will define supported workstation platform classes. Functional parity among these platforms will be implemented where practical.

WS.3 Workstation configurations will be standardized and centrally administered.

In order to facilitate use, sharing, and manageability, the workstation must meet defined minimum standards for hardware, software, and configuration. System software products, including the operating system, network operating system, graphical user interface, and connectivity software, will be standardized at the product version level, documented, and maintained under configuration control.

WS.4 Workstation local storage will be used primarily for system software.

While it is desirable from a manageability standpoint to run as much software as possible from file servers, practical considerations dictate that operating system software, graphical user interface software, and software which may perform excessive memory-to-disk swapping be loaded on the local workstation disk.

WS.5 Mandatory updates to workstation files will occur automatically at startup.

When a user starts up a workstation, it will automatically attach to the assigned file server. The workstation revision level is then checked, and, if necessary, the standardized part of the workstation will be automatically updated. This approach guarantees that the workstation will be current and correct without requiring central support.
WS.6 Workstations will implement standardized graphical user interfaces.

The *Computing Architecture* specifies that future applications will conform to site standards for graphical user interfaces. A native or dominant proprietary graphical user interface will be implemented on each workstation platform to provide ease of use and to support these future applications. The defined graphical user interface for a supported workstation type, the basic application services, and some user interface preferences of a system nature will be standardized.

WS.7 Workstations will support X-Windows as a least common denominator graphics-delivery mechanism.

Because X-Windows is client-server based, is layered upon TCP/IP, and is available on most host and workstation platforms, it will be supported as a "least common denominator" graphics mechanism. Standard graphical user interfaces will support X-Windows via an emulation application where necessary.

WS.8 Mandatory updates to user-specific system support files will be performed automatically at login.

When a user logs into a server, the revision level of the user's files will be checked. When necessary, automatic updates may be performed. For example, a user preferences file may require updating when a new software version is installed.
Information Servers

Description

Information server is a broad descriptor which includes all systems other than file servers and workstations. These may be database servers, computing engines, or other systems processing interactive and non-interactive applications. These servers may vary in size and configuration (from mid-range systems to mainframes) depending upon the type of information being processed. If specific categories of information servers and associated principles are defined (e.g., workgroup database servers), they will be categorized separately in future versions of this document.

Principles

IS.1 Information servers will support OSF/DCE.

The Open Software Foundation Distributed Computing Environment (OSF/DCE) covers a wide range of communications services supporting a client-server infrastructure. The services include a Distributed File System (DFS), remote procedure call (RPC), directory service, time service, security service (Kerberos), and threads.

IS.2 Business and office information servers will be centrally administered.

Business and office information servers are generally site-wide in scope and are best managed centrally.

IS.3 Manufacturing/process-control information servers will be administered by line organizations.

Manufacturing/process-control information servers are generally specific to an operating area or organization, and are best administered under local control.

IS.4 System operations will be automated where practical.

Software will be used to monitor systems, filter and act upon console messages, etc. to reduce the amount of operator interaction required.
Peripherals

Description

Peripherals include input/output devices such as printers, plotters, scanners, slide makers, aperture card readers, microfilm printers, etc.

Principles

PP.1 Standard peripherals will be distributed and readily accessible.

Attempts will be made to distribute common peripherals (LaserWriters, HP printers) conveniently close to the user population. Less common peripherals such as scanners, specialized printers (E-size or color, for example), plotters, slide makers, etc. will be installed in major population areas, not just in a central location. There may be authorization limits to control who can access specialized peripherals.

PP.2 Standard input and output media will be defined, and the use of non-standard media will be limited.

Available media (e.g., slides, aperture cards, microfiche, etc.) will be standardized, with the appropriate use of each type being defined.

PP.3 Office peripherals will be accessible from all supported workstation types and from all information servers.

It is more cost effective for peripherals to be sharable from multiple sources than to require redundant installations to support each platform. It is also more cost-effective to share peripherals among users than to have "personal" devices.

PP.4 Office peripherals will have direct network connections.

*Wherever possible, sharable peripherals will have direct Ethernet connection to the site network. This practice reduces the cost and improves the manageability by eliminating superfluous equipment such as print servers and Fastpath gateways, and improves performance over direct workstation attachment.
Electronic Documents

Description

Support for electronic documents (i.e., documents whose content is stored electronically) is considered part of the computing infrastructure because documents are the primary information exchange mechanism. (For the purpose of this section, electronic mail is not considered an electronic document; it is dealt with in a subsequent section.) Electronic document principles deal primarily with storage and access.

Principles

ED.1 Documents may be composed of multiple files.

A document may be composed of multiple files for any number of reasons: segmentation into separate files for each chapter, or inclusion of original spreadsheet or graphics files along with the word processing document. All components should be stored together for subsequent retrieval and revision.

ED.2 The preferred storage format for a document file is the native format produced by the product or application which created it.

The native format is the richest and therefore contains the most information.

ED.3 A document may be stored in multiple formats for specific purposes.

Some documents may be stored in both revisable and non-revisable form for revising, viewing, printing, markup, etc. For example, a CADD drawing may be stored in both vector and raster format.

ED.4 Documents will not be stored in obsolete file formats.

The set of site standards applications and/or their corresponding file formats will evolve over time as the marketplace and industry dictate. In some cases, conversions of documents will be required to ensure their continued usability. Infrastructure will be put in place so that when this situation occurs, users will automatically be provided ample notification of files which must be revisited and either updated or discarded.

ED.5 The ability to access (i.e., locate, view, and print) an electronic document will not be workstation-dependent.

The ability to access a document should not be dependent upon the type of workstation being used, provided the workstation is a standard, supported configuration.
ED.6 Documents will be divided into the following categories: private, workgroup, and managed.

Private documents are those which are used by an individual; workgroup documents are controlled by a workgroup administrator but have no indexing information; managed documents are access-controlled with stored indexing information.

ED.7 By default, private documents will be stored on file servers within the data space of individual users.

It is important to encourage users to place data into the reliable and secured network file space rather than on local storage. This will be accomplished by setting the initial defaults of all standard applications to direct data to the network unless otherwise specified and will be reinforced through training.

ED.8 Workgroup documents will be stored on file servers within a workgroup space.

Workgroups will be able to utilize the data space on workgroup file servers to store and informally share documents.
Desktop Office Products

Description

Documents are produced primarily by end-user tools which execute at the workstation level and provide basic office information processing functionality. These desktop office products are typically off-the-shelf software products which produce standard format files which are then stored on file servers.

Principles

DP.1 Desktop office products will support data interchange between all supported workstation platforms.

The standard products selected for a given functional area (e.g., word processing, spreadsheet, graphics, etc.) for one workstation platform must support file level data interchange with the comparable product selected for the other supported workstation platforms. For example, if product A is the standard word processor for type X workstations, the output file it produces must be readable by product B, which is the standard word processor for type Y workstations.

DP.2 Desktop office products will adhere to the graphical user interface standards of the workstation platform on which they execute.

The look and feel of desktop products will be consistent with that of the native workstation user interface to provide the benefits of a uniform desktop which include a reduced learning curve and easier support.

DP.3 Configuration files for desktop office products will have defined standard and personal components.

Within each standard application, the operating parameters which should be site-standard (such as keyboard maps or conversion attributes) will be maintained by the systems, while user-specific preferences will be stored in the user's private data space. If needed, the application configuration will be verified prior to activation of the applications. Commercial vendors will be encouraged to provide software with suitable configuration controls. Site-developed applications will be written to accommodate both site and personal configuration aspects.

DP.4 Site standard desktop office products will be defined for processing each document file format.

Each document file format (spreadsheet, word processing, image, etc.) will have a site standard desktop office product associated with it.
DP.5  A desktop office product will be available to provide character recognition for raster image files.

Character recognition will be provided as a utility independent of scanner hardware or software so that it can be applied to a raster image file at any time.
Document Management

Description

Document management is a method of managing and tracking the generation, revision, storage, and distribution of documents for which formal control over these activities is mandated or desired.

Principles

DM.1 The document content and specific indexing information will be stored electronically for all managed documents.

At a minimum, the content, author, and an identification will be stored. Ideally, content is revisable form, including illustrations, text, graphics, charts, formulas, etc.

DM.2 The indexing information for managed documents will be stored on information servers.

Indexing information for documents which require formal management will be stored on information servers.

DM.3 Access to content and indexing information of managed documents will be controlled; changes to either will be controlled to ensure they are synchronized.

It is critical that the document indexing information accurately represents the content, and that all updates to a document or its indexing information are authorized.

DM.4 Document management facilities will be available to all users.

Access to document management functions will not be centralized in a single group, though access to selected functions and documents will be restricted. Users will be able to submit for management any document created using a site standard application.

DM.5 Manual entry of indexing information which is duplicated within the content of a managed document will be minimized.

Where possible, indexing information will be automatically captured or derived from the content of a document.

DM.6 The primary search mechanism for managed documents will be indexing information; all managed documents containing textual information will be capable of being content-searched.
Managed documents will be located primarily through a search of the stored indexing information. Where appropriate, full text search of the document content will be used as a secondary mechanism for exact or alternate searches.

DM.7 The originator will be the primary entry point for the content and indexing information for managed documents (rather than a records indexing group).

Users will be individually responsible for providing the appropriate indexing information when submitting a managed document.

DM.8 The storage and indexing mechanism for managed documents will not attempt to maintain active live links.

Since linked documents attempt to use the data from one document as part of another document (so that as the data in the first document changes, the data in the second will automatically be updated), live links require that the secondary file be able to automatically locate and access the first file. Implementation of this approach is difficult and does not adhere to document revision guidelines. Therefore, files referenced by live links from managed documents must be duplicated for storage as independent components of those documents.

DM.9 Managed documents will have a definitive sensitivity determination.

Managed documents will have a preliminary sensitivity determination made by the provider when the content is submitted for management; those documents which are not initially determined to be non-sensitive will be treated as sensitive until an Authorized Derivative Classifier (ADC) or other appropriate reviewing official makes a definitive determination.

DM.10 Managed documents will be printed only upon user request.

Routine paper distributions of managed documents will be minimized; routine notifications of update will occur electronically.
Electronic Routing

Description

Electronic routing refers to the mechanism for electronically performing the review required for business documents and forms. Routing includes mechanisms for specifying reviewers, providing reviewers access to the review item(s), and querying the status of a routing item.

Principles

ER.1 There will be a single site mechanism to handle all electronic routing.

Rather than have each application which produces documents requiring routing implement its own mechanism, a central electronic routing mechanism will be implemented.

ER.2 Routing items will include documents, drawings, and forms-based information.

Routing items may include managed documents (word processing files, spreadsheets, slide presentations, CADD drawings, etc.) but may also include files representing purchase requisitions, travel request forms, Human Resources forms, etc.

ER.3 Access to content, routing information, and status information of all electronic routing items will be controlled.

It is important that the item, its routing sheet, and its status information be protected from unauthorized access.

ER.4 Item manipulation will be external to the electronic routing system.

Item manipulation, such as creation, editing, printing, viewing, or markup, will be performed using standard desktop office product or other applications. It is not a part of the electronic routing system.

ER.5 Audit trails will be maintainable for actions which alter the status of an item which is routing.

The electronic routing system must be auditable.

ER.6 Status information will dynamically reflect changes to the status of an item which is routing.

Timely status information is an essential component of electronic routing.

ER.7 The routing system will utilize electronic mail for notification of required actions.
The electronic routing system will send notices (such as requests to review documents) to users via electronic mail. This avoids the users' having to consult multiple sources by helping to centralize all important communications around a single facility—electronic mail.

**ER.8** Electronic routing will utilize directory services.

The purpose of directory services is to provide a single source for address information. Electronic routing should utilize this service rather than implementing a redundant solution.

**ER.9** Users will submit routing items via the workstation client; an interface for server-based submittal will also be provided.

Users will submit workstation-created items via the routing client component. There will also be an interface through which server-based applications can submit items for routing.
Electronic Mail

Description

Electronic mail is a key office computing application which will become even more critical as mail-enabled applications (such as electronic calendaring, conferencing, etc.) mature. Over time, the site mail environment will evolve from a terminal-host implementation to a client-server implementation.

Principles

EM.1 Users will have access to their electronic mailbox from any supported workstation.

This approach will allow a user to access mail from any workstation type and from any network location.

EM.2 Applications which interface with mail will do so via standard/guidedlined technologies.

Adherence to standard/guidedlined technology, such as mail application programming interfaces, will improve the portability of mail-enabled applications. Standard/guidedlined technologies are defined in Reference 5.

EM.3 Electronic mail will utilize directory services.

Electronic mail will be interfaced with the common directory services.

EM.4 Electronic message exchange with non-SRS locations will be done using standard/guidedlined technologies for data interchange.

This will reduce costs associated with implementing and supporting custom interfaces. Standard/guidedlined technologies are defined in Reference 5.
Directory Services

Description
Directory services provides a list of all personnel and their electronic addresses.

Principles

DS.1 Directory services will allow users to address mail interactively to any user on the site network.

DS.2 Directory information will be physically distributed to enhance reliability and performance.

Physical distribution is preferable to centralization because of the frequency of access and the potential impact of the information being unavailable.

DS.3 Distributed directories will be synchronized at least daily.

Timely directory information is essential.

DS.4 Site standard naming conventions will be developed.

Names must be established using a common scheme to ensure uniqueness and to adhere to addressing conventions imposed by external connections (e.g., the Internet, DOE, etc.).

DS.5 Electronic directory exchange with non-SRS locations will be done using standard/guidelined technologies for data interchange and will comply with security requirements for non-SRS access.

This practice will reduce costs associated with implementing and supporting custom interfaces. Standard/guidelined technologies are defined in Reference 5.
Figures

The architecture is further clarified through the following figures:

Network Schematic  *Illustrates the major components of the site network topology.*

File Server Connections  *Illustrates connections between workstations and file servers based upon user location.*
Network Schematic

Description

This figure illustrates the major components of the site network topology. An FDDI ring in the Central Computer Facility provides a high-speed interconnection between the mainframe systems. The ring is connected to the site Ethernet network through a router. The CCF IBM system is also connected to an Apex Token Ring which supports the connection of remote SNA devices, such as printers. Workstations and printers are typically Ethernet-attached via 10BaseT connections, although some high-performance workstations may have direct FDDI connections. Remote sites will be connected via T3 or faster circuits between routers.

Figure
File Server Connections

Description

This figure illustrates the file server connection a typical user would have when working from various locations. Note that when the user is outside his or her home sub-network (territory), the user continues to have access to personal and workgroup data, but system files (such as application programs) come from within the sub-network to reduce network traffic.

Figure
Scenarios

The architecture is further illustrated through the following scenarios:

Network Installation  
*Describes the process for upgrading the network in existing facilities.*

File Server and Workstation Environment  
*Describes the interactions between the user, workstation, and file server during normal login, application use, and file access.*

Peripheral Use  
*Describes the use of network-attached office peripherals*

Applications Platform  
*Describes the interaction between applications and platforms*

Workgroup and Managed Documents  
*Clarifies the creation of an informal document in a workgroup setting and the subsequent submittal to a document management system*

Document Review  
*Describes the process for electronically routing a procedure for review.*

Document Index Searching  
*Provides an example of how the document index can be used in an engineering environment.*
File Server and Workstation Environment

Description
This scenario describes the interactions of the user, workstation, and file server in a standardized integrated workstation environment:

Scenario
Bill comes into work and turns on his workstation. When the system boots, it automatically connects to the territorial file server to which it is assigned. The revision level of the workstation is then checked, and any necessary updates to the workstation system software are automatically copied to the workstation. The workstation then presents a log-in screen. Bill enters his ID and password, and is logged in to the network. He is automatically connected to the file server containing his personal data space, as well as the three servers which he routinely uses to access workgroup files. His personal configuration information is used to customize his environment (colors, etc.) and his graphical user interface desktop appears.

The desktop contains icons for the site standard desktop office products and applications. Bill clicks on the word processor icon, and the application, which is stored on the file server, is copied into memory on the workstation and begins execution. It reads Bill's preferences file from his private data space, as well as the system-wide preferences file contained on the system space of the file server, and opens a window. Bill creates his document, and saves it. By default it is stored in his private space on the server. Because this space is protected by Bill's password, he is assured that this information will be secure.

Bill is interrupted by a phone call requesting him to bring some papers to a meeting down the hall. Because there is no computer activity for a few minutes, the workstation drops to a screen saver, hiding his information from view. When he returns, Bill enters his password to clear the screen saver and continue working. Next, Bill clicks on an icon which corresponds to an application used only by his workgroup. The application, stored on the workgroup server, launches. Bill does his work, storing the output on the workgroup server for others to access. He then logs out, returning the display to the login screen.

Later that afternoon, Bill travels across site to meet with Bob. Bob has a different type of workstation than Bill, although both are supported. During their discussion, a question arises about the document which Bill had created that morning. Bill decides to check the document using Bob's workstation. Bob logs out and when the login screen appears, Bill enters his ID and password. His is then connected to the file server containing his personal files, as well as the three servers containing workgroup files, just as if he were in his office on his usual workstation. The only difference is that the applications are now coming from the server to which Bob's workstation is assigned in order to minimize network traffic. Since all file servers have the same software but Bill's personal preferences come from his space, the difference is imperceptible. Bill opens the document using the word processor for his workstation and discusses the content with Bob. He is able to do this easily because the standard application is nearly identical on both types of workstations.
Peripheral Use

Description
This scenario describes the use of network-attached office peripherals.

Scenario
Bill opens his word processing document and directs it to the closest laser printer (which is about 20 feet away). The files are queued through the territorial server which provides service to Bill's workstation and begins to print. The phone rings—it's Bill's boss. He's in another building and needs a copy of Bill's project schedule. Bill directs it to the C-size plotter in a room near his boss's meeting. Since the plotter is on the network, it is easy for Bill to select the device, and the download goes quickly. And because it's a standard device, Bill is confident that the chart will print correctly.
Applications Platform

Description

This scenario describes the interaction between applications and platforms.

Scenario

A new application has been developed according to the client-server model. It consists of a client component for each of the standard workstations types and a server component which executes on one of the information servers. The two components communicate via OSF/DCE remote procedure calls using TCP/IP transport.

The interaction of the client and information server components was tested using the information server testbed. The client components of the application (one for each supported workstation) were then distributed to the system volume of the territorial servers where they are accessible to all users when they log into the network. Each of the standard workstation clients utilizes the “native” graphical user interface and communication facilities provided by the standard workstation platform.
Network Installation

Description

This scenario describes the steps necessary to upgrade the network environment within an existing facility to the specified standard configuration:

Scenario

The network is being upgraded in an office building onsite. Two trailers near this building are to be included in the upgrade. Universal wiring has been installed for the 450 cubicles/offices in the building and in the trailers, although it is currently used only for serial terminal server connections. When the networking team begins design of the modifications, the first thing they do is to logically divide the building into sub-networks. They decide on three sub-networks of 150 each—one for each hallway in the building. Because the two trailers have only a small number of offices, they decide to include them in the sub-network associated with that part of the building closest to the trailers. That keeps each sub-network below the 200 workstation limit and aligns it with a natural boundary. The team next installs 10BaseT hubs which are connected to the universal wiring. The hubs for an individual segment are interconnected via Ethernet. Each sub-net consists of one or more hubs connected together over an Ethernet segment. Each sub-net is then attached to a multiprotocol router. The router is in turn connected to additional telecommunications equipment providing a T3 circuit to the central telecommunications facility.

A file server is installed on each sub-network, and Ethernet cards are installed in the workstations. As this is done, the universal wiring for those workstations is transferred from terminal servers to 10BaseT hub Ethernet connections. TCP/IP address ranges for each sub-net are activated on the BootP server software which is loaded on each file server. As each workstation is installed, the BootP server assigns and registers a unique IP address corresponding to the Ethernet card address. Later, the data table will be downloaded to maintain address information for security purposes.

A few weeks after the initial installation, several engineers in the building acquire high-performance workstations and request FDDI connections to permit high-speed data sharing between those systems. The network team installs an FDDI concentrator in the wiring closet, connects it to the router, and switches the universal wiring connection from the 10BaseT hub to the FDDI concentrator. The FDDI interfaces in the workstations are connected to the FDDI hub via the universal wiring connection.
Workgroup and Managed Documents

Description

This scenario describes the creation of an informal document in a workgroup setting and the subsequent submittal to a document management system.

Scenario

Bill creates a word processing document requesting a summer intern using his workstation and saves the document on a workgroup server. He then sends mail to the other members of his group telling them that the document is available, if they would like to add to the justification. Jane, who is in Bill's group, uses the site standard word processor for her workstation type to open the document. She makes several modifications, saves the document back to the server, and prints a copy on the network-attached printer down the hall. She also saves a copy in her private data space so that she can use it as a starting point to begin preparing the intern's assignment list.

Later in the week, Bill decides that the justification is complete and ready to be given to the Human Resources representative. Jane suggests that although it's not mandatory for this type of document, it would be a good idea to submit the justification to the document management system. That way, it can be easily located either when the summer student arrives or next year when someone else wants to request a summer intern. Bill clicks on the document management icon on his desktop and selects the "submit" option. He is then prompted to select the document to be submitted and to indicate the appropriate document type. The document management system automatically creates an index record for the document, containing Bill's name, the date, the document type, the document title, the required retention period, and a set of keywords based upon a text scan of the content. Bill next sets access rights for the document; he indicates that anyone may read the document, but only his workgroup may revise it. He also requests that the Human Resources representative be automatically notified that the document is available. The justification is then moved from the workgroup space to the nearest document management server.
Document Review

Description

This scenario illustrates the process for electronically performing the review and approval of a draft procedure.

Scenario

Bob has been assigned the task of preparing a new operating procedure. Using the site standard word processor, he creates a draft and saves it in his private space on the file server. He then creates several figures using the standard graphics package, saves them in his file space, and pastes copies into the draft document. Bob then clicks on the document management icon on his desktop and selects the graphics files as well as the word processing file for submission. That way, the original graphics will be available for revision at a later date along with the text. Bob then chooses the "procedure" document type, enters the appropriate indexing information, and specifies the proper access rights. The files are then moved to the document management server.

Next, Bob requests that the document be routed for review and approval. The system automatically knows the proper routing list for the procedure based upon its type and author. Jane, the first person on the approval list, receives notification that the document requires her review. Through the document management application, she requests a copy for markup. Copies of the document files are staged to her private data space on the file server. When Jane clicks on the copy of the procedure, the site standard word processor launches automatically and opens the file. Jane scrolls through the document until she finds a step which is incorrect. She selects the text, opens a new word processing window, pastes the text, and makes corrections. She also includes an explanatory paragraph indicating why the original step was unacceptable.

Finished with her review, Jane saves her correction into a new file and exits the word processor. She then clicks on the document management window on her desktop and uses the "review" option to indicate that she has made a comment which requires disposition and that she has completed her review. She then indicates to the document management application which file contains her comments. At that point, the application deletes the review copies of the document files from her data space, moves the comment file to the document management server, and continues with the "routing" of the procedure.
**Document Index Searching**

**Description**
This scenario illustrates the use of the document index in an engineering environment.

**Scenario**
Bill has been assigned the task of reviewing the design of a control system located within a facility he supports which appears to have a grounding problem. The system was installed several years ago, before Bill came to the site, so he is not familiar with its history. He clicks on the document management application icon and selects the "Index Search" option. He requests a search for documents with the facility name within the title field. The system finds 250 drawings and 25 other documents. Somewhat surprised at the number of documents returned, Bill decides to narrow the search by clicking on the result and selecting the "Full Text" search option. He searches for "control systems or grounding" which results in 2 documents being found. He then selects the option which requests that informational copies of those documents be transferred to his private data space so that he can view and/or print them.
DATE
FILMED
9/14/93
END