Section 1
Operator Environment

This section gives you an overview of the operator environment by introducing the hardware, concepts, and tools you need to operate the system effectively. It describes the responsibilities that are typically handled by the system operator, provides an overview of the system hardware, and introduces the system software. Detailed information about the hardware and software is available in other manuals. Refer to the manuals listed in Appendix B.

For more ref see 1.4

www.google.com

1.1. About This Manual

This manual describes operator responsibilities and procedures for OS 2200 systems. It provides basic concepts and objectives of system operations and gives specific operating procedures.

Documentation Updates

This document contains all the information that was available at the time of publication. Changes identified after release of this document are included in problem list entry (PLE) xxxxxxxx. To obtain a copy of the PLE, contact your Unisys service representative or access the current PLE from the Unisys Product Support Web site:

http://www.support.unisys.com/all/ple/xxxxxxxx

Note: *If you are not logged into the Product Support site, you will be asked to do so.*

Audience

System operators are the primary audience for this manual. System administrators and programmers might also need to read and refer to this manual.

Anyone using this manual must be familiar with mainframe computer operation and terminology, and have a basic understanding of Executive Control Language (ECL) and File Utility Routines/Program File Utility Routines (FURPUR).

How to Use This Manual

This manual is designed to be used primarily as a reference. Sections 1 through 9 include the basic concepts and objectives of system operation and specific operating procedures. Section 10 lists the unsolicited keyins according to function, and Section 11 provides detailed information about each keyin.

The *System Console Messages Reference Manual* must be used in conjunction with this manual. It lists and explains console messages, provides system error codes, and describes other types of errors.

Notation Conventions

This manual uses these conventions for keyins and messages:

- Uppercase letters

  Indicates the exact name of the operator command, also known as a *keyin*, for example: UP

- Uppercase letters with underscores

  Indicates a system generation parameter, for example: SENTRY_CONTROL

- Lowercase italicized letters

  Indicates a variable name, for example: *cmod*

- Leading zero on addresses

  Indicates an octal address, for example: 077

- Small braces and bar

  Indicates that the parameter can have one of two values, for example: {UPIDN}

- Brackets

  Indicates optional parameter, for example: [,*options*]

- Brackets and bar

  Indicates optional parameter; you can select one of the indicated values for example [STDISHARED]

- Subscript numbers on variable names

  Denotes that there can be several values for the same parameter, for example: devnam_1

- Ellipsis (...)

  Indicates that more values for the same parameter can be added, for example: $\mathit{devnam}_1,\mathit{devnam}_2,\ldots,\mathit{devnam}_n$

Variable Names

Following is a list of the most common variable names used throughout this manual.

Symbolic Name	Meaning
Cmod	channel module
Cu	control unit
Devnam	device name
dir-id	directory identifier (for example, SHARED# or STD#)
F-cycle	file cycle
host-id	host identifier (for example, A, B, C, and so forth)
iop	input/output processor
ip	instruction processor
mmod	memory module
pack-id	pack identifier
run-id	run identifier
site-id	site identifier
sname	symbiont name
user-id	user identifier

This is an example of a keyin using a variable name:

```
DN ip
```

1.2. Operator Responsibilities

The operator responsibilities described here relate to a Unisys OS 2200 system. Although this manual contains specific information to adequately perform some of the responsibilities, you have to refer to other Unisys publications for detailed information.

The operator responsibilities for a Unisys system include the following:

- Initialize the system software and install and initialize products and application software

  System start-up and initialization is the process that brings a system to the ready state. It includes powering up system components and loading software. Section 3 provides general information about system start-up and references manuals that contain specific information for some systems. See Section 8 for system security file initialization procedures.

- Respond to system messages

  System messages are sent to the system console to inform the operator of system activity or to request that the operator perform some action, such as loading a specific tape. Section 2 includes information about the system console, system messages, and other aspects of console operation.

- Enter jobs into the system and check their status

  This activity is done as part of monitoring system operations and in response to requests from system users. Section 4 includes an overview of the keyins used for controlling job input and checking their status.

- Monitor system status and throughput

  General system status information is continuously displayed on the system console. Keyins let the operator display more detailed information, make entries in the system log concerning system activity, and adjust the job mix for efficient operation. The status of system components, such as printers (and their print queues) and disks (and storage allocation), is displayed in response to keyins. Section 4 includes information about the keyins used for status and throughput operations.

- Mount and dismount tapes

  Tapes are mounted and dismounted in response to system messages. Section 5 describes how to respond to tape messages and includes information on Tape Automatic Volume Recognition (TAVR), a feature that lets the operator mount (premount) tapes before they are requested.

- Prep disks

  Disks can be either fixed or removable. They can be reserved for specific assignments, and removable disks can be removed from one system and put on another. Information about disk packs and keyins used with disks is included in Section 5.

- Collect and sort printed output

  If your system is configured to label user printouts, see Section 8.

- Back up system software

  Backing up system software on a regular basis minimizes damage that can be done by system crashes, failed recoveries, and other system problems. It lets you recover more quickly and with greater confidence. See the *FAS Operations Guide* for more information on doing system software backups.

- Dump memory

  System dumps can be performed to troubleshoot system errors. They can be started either manually or automatically. Section 6 describes the procedures for performing and processing system dumps.

- Recover the system if it fails

  Recovery of the system generally refers to software recovery after a system failure. Integrated recovery and the integrated recovery utility, as well as audit trails, are some of the features that streamline system recovery. Section 3 describes general recovery procedures and Section 7 provides information on audit trails and step control options, which are used in integrated recovery.

In addition to the tasks just listed, you need to be familiar with the following:

- Objectives, procedures, and standards at your site
- Efficient operation of hardware components
- Input, output, and processing requirements of the operating system
- Recognizing inefficient system operation and determining corrective action
- System operations in a multihost operations environment and how it differs from a one-host environment, if your site has a multihost environment.

1.3. System Hardware Components

Operating a Unisys computer system requires you to interact with the system hardware in a variety of ways: system start-up, system shutdown, loading tapes, preparing disks, and so on. This subsection provides a general overview of system hardware, identifying the components and their function. Specific information about powering on the components, identifying the location of switches and indicators, and so on is covered in the hardware manuals shipped with the component.

1.3.1. Central Electronics Complex (CEC)

The two major components of a central electronic complex (CEC) are the processing complex and the I/O complex, described below. The system can optionally contain an Extended Transaction Processor (XPC). Refer to the *XPC Operations Guide* for more information.

Processing Complex

The processing complex contains Processing Complex Cabinets (PCC), Processor Cooling Units (PCU), and Modular Power Centers (MPC) or Power Peripheral Distribution units (PPDU).

Each processing complex cabinet contains

- Instruction processors: The instruction processor executes program and system software instructions.
- Storage controller: The storage controller interfaces the instruction processors and the I/O complex with main storage. Storage controllers allow multiple PCCs and I/O complex cabinets to be configured as balanced multiprocessor systems.

- Main Storage Units (MSU): Each storage controller has a direct interface with two independent MSUs.
- Network Interface Module (NIM): The NIM connects the PCC with the system control facility for system operations.

The processing complex also contains the processor cooling unit and the modular power center. The PCU provides liquid cooling for the PCC, circulating water cooled by an external source. One PCU is required for each PCC.

The MPC or PPDU provides an isolation transformer, circuit breakers, and voltage-matching facilities for the central electronics complex.

I/O Complex

The I/O complex includes I/O complex cabinets (ICC) and disk subsystem adapter cabinets (DSAC). These units provide the system interface and the I/O channels to support peripheral equipment. The channels provide the final hardware link to the disk, tape, printer, and communications peripherals. They also manage and control transfers to and from the peripherals.

Each I/O complex cabinet contains

- I/O remote adapter: The I/O remote adapter provides the main storage interface to the ICC.
- I/O processor modules: I/O processor modules control the initiation, transfer, and termination of data sequences to specific channels in the ICC.
- Block multiplexer channel interfaces: BMCs provide the final hardware link to the disk, tape, printers, and communications peripherals. They manage and control transfers to and from the peripherals.
- An interface for each ICC to support one optional DSAC.

Each DSAC contains word channel modules used for the connection and control of peripheral devices requiring word channel interfaces.

See your *System Capabilities Overview* for more information.

1.3.2. Extended Processing Complex (XPC-L)

Extended Processing Complex (XPC-L) is an optional hardware device that connects to all hosts in an Extended Transaction Capacity (XTC) system. In a one-host system, file and record locking is handled through software locking by TIP file control for TIP files or by UDS Control for UDS/TIP files. In an XTC system, XPC-L provides hardware locking outside the hosts to allow access to shared databases regardless of the database type. In addition, the XPC-L provides interhost communications.

1.3.3. Server Sentinel

The Server Sentinel software provides system control processing. Server Sentinel software executes on the embedded Service Processors.

Through the CSE, which provides access to hardware, the Server Sentinel software also communicates with the OS 2200 operating system and the CEC hardware.

1.3.4. Peripheral Subsystems

The peripheral subsystems provide data storage and hard-copy output for user programs. Data storage is provided by tape subsystems and disk subsystems (mass storage). Printer subsystems provide hard-copy output.

Mass Storage (Disk Subsystems)

Disk subsystems consist of the control units and their attached disk devices. The components of the disk subsystem are available in many configurations to meet a wide variety of needs.

For specific information about the disk subsystem attached to your system, refer to the manuals provided with it.

Tape Subsystems

Tape subsystems consist of the control units and their attached tape devices. Like disk subsystems, they are available in many configurations to meet a wide variety of needs. There are different types of tape devices and control units to handle reel and cartridge tapes of different densities.

Section 5 contains information about the cartridge tape library (CTL), Tape Automatic Volume Recognition (TAVR), and the tape subsystem. Refer to documentation provided with the tape subsystem components for more information.

1.3.5. Communications Subsystems

OS 2200 systems can include

- CSIOP, which is driven by CMS 1100. The following network connection devices can be attached to the CSIOP:
  - Block Multiplexer Channel (BMC) for connection to a Distributed Communications Processor (DCP).
  - Chan-0 Adapter (C0CA) for connection to a local area network. Ethernet and FDDI are available.
- PCIOP, which is driven by the CPComm software product. Ethernet network interface cards and FDDI network interface cards can be attached to the PCIOP.

1.4. System Software

System software includes the operating system of which the Exec is a part, and the various utilities, tools, and diagnostics that keep the system running so that user programs run properly. This manual documents the Exec and its features as they relate to system operation.

The Exec controls the system operating environment. It processes runs, controls files, manages system resources, and performs input/output operations for users. Console software lets the operator interact with the Exec, through operator keyins, to monitor and control system operation.

The following subsections describe some of the Exec features you need to understand as an operator. Your system cannot have all these features because some of them are optional.

1.4.1. Operating System and the Exec

The OS 2200 operating system supports batch, interactive, and transaction processing.

The Exec provides the basic support for all central complex hardware and channel-connected peripherals. It also isolates user programs from direct interface with the hardware. At its lowest level, the Exec makes users aware of the hardware and lets them control it. Unisys device control software, such as Enterprise Output Manager, the printer control program, and the online diagnostic software generally use this level of interface. In higher level operations, the Exec takes complete control. Interfaces for tapes and disks, for example, do not require the user program to know the physical device characteristics at all.

The Exec also controls how system resources are allocated. The primary resources are memory space, instruction processor time, mass storage space, tape drive and printer allocation, and network channels. Once resources are allocated, the Exec makes sure that programs do not interfere with one another or simultaneously modify the same data.

Common security and limit controls are also handled by the Exec. Security prevents unauthorized access to programs or data. Limit controls (the Quota system) make certain that no single user exceeds the resource usage limits imposed by the system administrator.

The operator keyins described in Section 11 let you control and modify the operational parameters of the operating system and request information from it.

1.4.2. Communications Software

A suite of software products enables communications between programs executing on the ClearPath system and software executing in other computers, work stations, and devices. Communications Platform (CPComm) and SILAS provide the network protocol handling and control of the network connections.

COMAPI provides a Sockets-like interface to CPComm and the network. CITA provides a TCP/IP path for TIP programs. The Message Control Bank (MCB) is the message handling and message recovery component of the OS 2200 integrated recovery system.

Figure 1-1 shows the relationships among CPComm, SILAS, and the other communications software components.

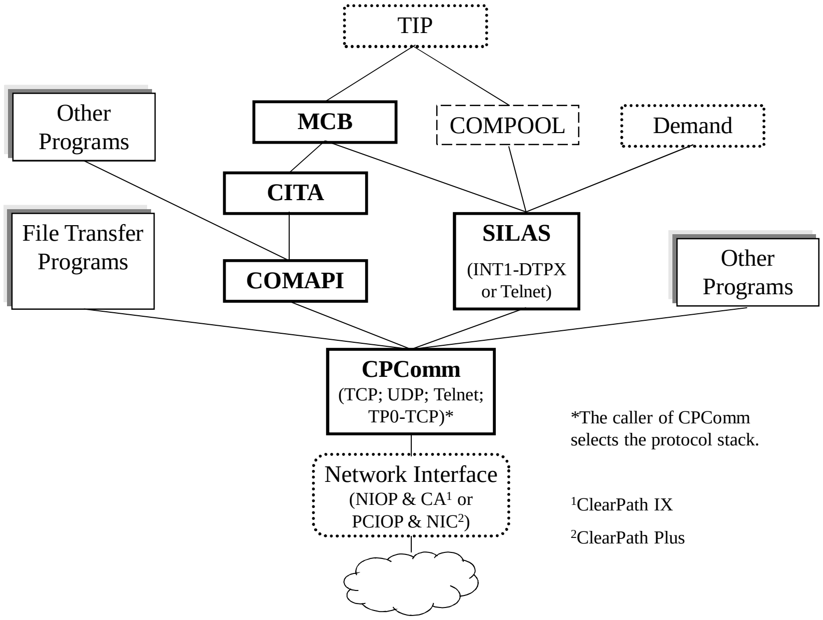

Figure 1–1. Communications Products with CPComm

Refer to the following documents for operational instructions for the communications software products:

- *Communications Platform Configuration and Operations Guide*
- *System Interface for Legacy Application Systems (SILAS) Configuration and Operations Guide*
- *Communications Application Program Interface User's Guide*
- *ClearPath Enterprise Servers Communications Interface for Transaction Applications Configuration and Operations Guide*
- *Message Control Bank (MCB) Administration and Operations Guide*

1.4.3. Transaction Processing (TIP)

Transaction Processing (referred to as TIP) is an extension of the Exec that provides a high-performance system in which a user causes the execution of a predefined transaction program by entering an input message from a remote terminal. The program typically accesses the application program database and returns a response to the user.

The Exec supports the creation and maintenance of the database and program files for these applications programs. Step control and audit control are important mechanisms for TIP that allow each program step to be completed and logged so that system failures do not jeopardize transactions.

For more information about TIP, refer to the *Transaction Processing Administration and Operations Reference Manual*.

1.4.4. Multi-Host File Sharing (MHFS)

Multi-host File Sharing (MHFS) is an Exec feature that allows file sharing between multiple OS 2200 systems. Each system in the MHFS environment is called a host. MHFS associates the files with a standard or shared master file directory and manages communications for file sharing within a host and across multiple hosts.

Keyins are available that enable you to change the MHFS configuration by bringing hosts or shared devices up or down. See Section 9 for operations procedures within a multihost environment. See the *MHFS Planning, Installation, and Operations Guide* for more information on MHFS.

1.4.5. Extended Transaction Capacity (XTC)

Extended Transaction Capacity (XTC) is an optional group of features that expands transaction processing capacity into multiple host systems. XTC provides for shared, synchronized, logical record access for multiple hosts between transactions and databases on shared mass storage. The application groups that simultaneously access the shared mass storage databases are called concurrent application groups. The XPC-L is a required central complex hardware device connected to all hosts in an XTC configuration that synchronizes locking for concurrent access to shared mass storage databases.

See Section 9 for operations procedures within a multihost environment. See the *XTC Planning, Migration, and Operations Guide* for more information on XTC.

1.4.6. Partitioned Applications (PA)

Partitioned Applications (PA) is an optional group of features that increases transaction processing availability. It operates in both one-host and two-host environment.

With a two-host Partitioned Applications environment, each host runs a different application group (or groups) with its database on shared mass storage. At the same time, each host can serves as a backup for application groups on the other host without affecting production or performance on either host.

The application groups for which backup support is provided are called switchable application groups. If a host fails or is brought down, its switchable applications groups are automatically moved to the other host. In addition to recovering switchable application groups on the other host, Partitioned Applications also allows application groups and components to be automatically recovered on the same host.

See Section 9 for more information on operations procedures within a multihost environment. See the *Partitioned Applications Conceptual Overview* for more information on Partitioned Applications.

1.4.7. Integrated Recovery

Integrated recovery synchronizes database and message recovery after a failure. Recovery features work in combination to expedite the recovery process, minimize recovery difficulties, regain system stability, and ensure data integrity. The major Exec components of integrated recovery are Exec step control, Exec audit control, and TIP file control.

Integrated recovery encompasses the features necessary to provide the database recovery needs of the Exec, TIP, and UDS, as well as the message recovery needs of MCB.

Integrated recovery is available only for user sessions or programs associated with an application group. When you reboot the system after a failure or after bringing the system down, the Exec initiates most of the necessary recovery actions for each application group. The Exec either determines the appropriate action or prompts you to define the appropriate action. When necessary, the Exec also prompts you to start the Integrated Recovery Utility (formerly IRU) short recovery to bring up an application group.

When the recovery action initiated by the Exec cannot recover the system to its previous state, Integrated Recovery Utility provides other methods to recover the system, such as medium or long recovery.

Refer to the *Integrated Recovery Conceptual Overview* for information about integrated recovery concepts and procedures.

Step Control

Step control is an Exec integrated recovery component that synchronizes database and message recovery activities for user programs associated with a particular application group. It also provides central control information for the application group’s integrated recovery software components so appropriate recovery actions can take place.

A step is a recoverable or nonrecoverable unit of work. It represents a portion of processing associated with a user program. A recoverable step is a unit of recoverable processing (for example, a sequence of user program commands that update a database). If a failure occurs before a recoverable step point is reached, the database updates associated with the step are discarded and the program rolls back (reverts) to the point just after the program’s last recoverable step.

Section 7 provides information on the step control initialization and recovery options.

Audit Control and Audit Trail

Audit control is an Exec component that initializes, creates, maintains, and controls access to an application group's audit trail. In addition, it manages audit trail recoveries and audit trail keyins. See Section 7 for audit control operations procedures.

An audit trail is a continuous and chronological sequence of audit records stored in mass storage or a tape file. In general, the audit record represents a recoverable event. Audit trails are associated with complexes within the Exec and manage all aspects of data storage on behalf of their associated complexes.

The complexes that use audit trails are:

- System log
- Integrated recovery step control
- Integrated recovery Transaction Performance Monitor (TPM)
- Capacity on Demand (COD)

Audit trails can be configured as simplex or duplex (one data file or two data files). Individual audit trails can also be configured to use tape or mass storage.

Integrated Recovery Utility

The Integrated Recovery Utility (IRU) plays a key role in an integrated recovery system. System software components such as the Exec, TIP file control, UDS, and MCB have built-in procedures to handle most failures. If these recovery features fail, however, you can use Integrated Recovery Utility to perform alternate recovery procedures.

IRU is a software tool that combines and uses information available from other integrated recovery components to recover files and databases to ensure their integrity. Often, the work IRU does depends on the success or failure of the other integrated recovery system components. IRU might be considered a contingency-action product in recovery situations. You use it when automatic safeguard or recovery actions of the other components fail.

IRU supports three environments: single-host, Partitioned Applications, and Extended Transaction Capacity (XTC). IRU also offers three methods of recovery: short, medium, and long. Refer to the *Integrated Recovery Utility Operations Guide* and the *Integrated Recovery Conceptual Overview* for complete information.

1.4.8. Security

Security is available in the following options:

- Fundamental Security

  Fundamental Security, a standard feature of OS 2200, offers basic protection for the ClearPath enterprise computing environment. Fundamental Security establishes security controls at the system level and provides limited security based on an individual user’s identity.

  Security Level 1 is an optional feature, which provides additional protections beyond Fundamental Security. Additional security levels (2 and 3) can provide an even more rigidly protected environment for sites with more stringent security requirements.

  The security officer is responsible for security administration and planning. If you have specific questions about security operations, ask your site’s security officer.

- Security Option 1

  Security Option 1 enhances Fundamental Security with security records, file ownership, file security, privileges, clearance levels, residue security, and object module subsystem entry point protection.

- Security Option 2

  Security Option 2 builds on Security Option 1 with compartment sets, tape volume security, symbolic clearance levels, TIP message security, print output labeling, and detection of improperly labeled and nonlabeled objects.

- Security Option 3

  Security Option 3 extends file protection, provides common bank protection, and controls terminal communications.

As a system operator, you need to know which option is installed at your site and you need to understand the impact it has on your responsibilities, primarily in booting the system, distributing printouts, and labeling tapes and mass storage files. You must also be certain you have the proper security privileges to perform operations with integrated recovery, use the TS keyin, and boot the system.

The security officer is responsible for security administration and planning. If you have specific questions about security operations, speak to your site’s security officer.

1.4.9. Unit Duplexing

Unit Duplexing is an Exec feature that reduces system vulnerability to mass storage failures. It consists of a hardware configuration in which each mass storage device has an associated backup device that is transparent to all end-user software and to most system software.

If a user program issues a request to read or write to a file on a unit-duplexed device, the write request is automatically performed on both devices and the read request is performed on either device. From a software point of view, the unit-duplexed devices are bit-for-bit identical.

For additional information, refer to the *Unit Duplexing Planning, Installation, and Operations Overview.*

1.5. Operator Profile

System administrators have the option of setting up an operator profile for the system operators through the security management product.

This operator profile consists of an array of strings, called environmental variables, which contain information that defines operators, applications, and the system. Included in this profile is an environmental variable that lets operators receive messages from the Extended Language Message System (ELMS) in their native language, or another language, as determined by the site. Exec messages are currently displayed only in English.

The profile is set up at system initialization time using the security management product. After system initialization, profile changes are made through an Exec call. Refer to the *TeamQuest SIMAN Administration and End Use Reference Manual* or the *System Services Programming Reference Manual* for more information.

The security administrator can use either of the following products. In this document, the term "security management product" refers to one of the following products:

- Security Administration for ClearPath OS 2200 includes a Security Client for creating and modifying system, application, and personal security records from a remote Windows workstation and an agent that runs on the Dorado server. Administrators use this application to configure security features, set up user IDs, and control access to system resources. Nonadministrators use it to view or modify their personal security records. A batch processor (@SECMGR) provides a batch/demand interface to perform those same administrator or end-user operations at an OS 2200 terminal. For more information, see the *Security Administration for ClearPath OS 2200 Help.*
- TeamQuest® Site Management Complex (SIMAN) provides a menu-driven interface for creating and maintaining security and resource control in an OS 2200 system. The SIMAN system accesses and uses any available OS 2200 terminal emulator. SIMAN includes a batch processor whose command syntax is compatible with @SECMGR. For more information, see the *TeamQuest Site Management Complex (SIMAN) Administration* and *End Use Reference Manual*.