# COMMUNICATIONS SUPPORT PROCESSOR

# (CSP)

# FUNCTIONAL DESCRIPTION MANUAL

2-FD-JUL 86-U-2
TR-85-43232-B004

SEPTEMBER 1985
REVISED MARCH 1986
REVISED JULY 1986

Prepared for

Rome Air Development Center
Air Force Systems Command
Griffis AFB, New York

and

Air Force Intelligence Service
Bolling AFB
Washington, D.C.

Prepared Under Contract No. F30602-85-C-0113
by Informatics General Corporation, Bellevue, Nebraska.

Declassified and Approved For Release 2013/02/13 : CIA-RDP89B01354R000200270011-9

# DOCUMENT CHANGE NOTICE FORM

CPCI: CSP SYSTEM DOCUMENT DATE: July 1986

DOCUMENT TITLE: CSP Functional Description

AFIS/IND LIBRARY CONTROL NUMBER: 2-FD-JUL86-U-2

INFORMATICS DOCUMENT CONTROL NUMBER: TR-85-43232-B004

**********

REASON FOR CHANGES TO DOCUMENT: _____
(I.E., CPR, CCR, SITE SURVEY, ETC.)

CSP RELEASE/UPDATE VERSION NUMBER: V2.4.5

DOCUMENT MODIFICATION AS FOLLOWS:

_____ NEW DOCUMENT - REPLACES ALL OTHERS SUBMITTED

_____ REVISION WITH CHANGE BARS

__X__ CHANGE PAGES WITH CHANGE BARS

IF REVISION, COMPLETE THE FOLLOWING:

| REMOVE | INSERT |
|---|---|
| iii | iii |
| 3-10 | 3-10 |
| 3-11 | 3-11, 3-11.1 |
| 3-42 | 3-42 |
| 3-43 | 3-43 |

# DOCUMENT CHANGE NOTICE FORM

CPCI: CSP SYSTEM DOCUMENT DATE: March, 1986

DOCUMENT TITLE: CSP Functional Description

AFIS/IND LIBRARY CONTROL NUMBER: 2-FD-MAR 86-U-1

INFORMATICS DOCUMENT CONTROL NUMBER: TR-85-43232-B004

**********

REASON FOR CHANGES TO DOCUMENT: _____
(I.E., CPR, CCR, SITE SURVEY, ETC.)

CSP RELEASE/UPDATE VERSION NUMBER: V2.4.4

DOCUMENT MODIFICATION AS FOLLOWS:

_____ NEW DOCUMENT - REPLACES ALL OTHERS SUBMITTED

__X__ REVISION WITH CHANGE BARS

_____ CHANGE PAGES WITH CHANGE BARS

IF REVISION, COMPLETE THE FOLLOWING:

| REMOVE | INSERT |
|---|---|
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |
| | |

# TABLE OF CONTENTS

PAGE

## LIST OF FIGURES

# SECTION 1. INTRODUCTION

This document is the Functional Description for the Communications Support Processor (CSP). The CSP is a computer system designed to automate the functions of a Telecommunications Center (TCC). Its development, distribution, and maintenance is under the auspices of AFIS/IND, Bolling Air Force Base, Washington, D.C. CSP is an element of the Common User's Baseline for the Intelligence Community (CUBIC). CUBIC serves as a single source for computer systems designed to automate nearly all phases of intelligence data handling functions.

## 1.1 Purpose

This manual serves two functions:

- To provide a complete directory and description of CSP functionality and services. As such, it may be viewed as a catalogue of standard and optional features provided by CSP.

- To aid management level design personnel in the decision making processing and to properly and completely evaluate CSP applicability and utility in proposed installations.

Since this manual is targeted towards design/planning level personnel, it is presented at a medium level of detail. This is the second of three documents comprising descriptive literature on the CSP. The CSP Overview presents the boradest view of CSP, while the CSP System Design Specifications presents the most detailed CSP discussion. Since CSP is an existing system, this manual is presented in lieu of a Functional Requirements Manual, which normally precedes system procurement or design and development.

## 1.2 Scope

This document covers the following aspects of CSP:

- A generic level description of CSP, its usual applications, and possible adaptations to specifications user needs.

- A semi-detailed description of all visible capabilities and functionalities of the system.

- A description of environment, both hardware and software, which can be directly translated into a procurement list.

- Discussion of the operational requirement of a CSP installation, including operator/user staffing, program maintenance, and management levels.

## 1.3 References

The following documentation is referred to in this manual or serves as an alternative source of information concerning various aspects of CSP design operation, maintenance, or procurement. The publications listed below have been prepared, whenever applicable, in accordance with DoD Standard 7935.1-S (Automated Data System Documentation Standards).

### 1.3.1 CSP Technical Documentation

These documents, previously developed, directly refer to CSP. They are available through official channels from AFIS/IND.

#### 1.3.1.1 CSP System Overview

Author/Source - Informatics General Corporation
Reference Number - TR-83-43110-07
Date - May 1983/Revised October 1984, March 1985 and May 1985
Security Classification - UNCLASSIFIED

The overview of the CSP is intended for use by management and systems personnel who require knowledge of its philosophy, background and capabilities. It provides a synopsis of CSP origins and objectives, status of CSP capabilities, system design and architecture, and future enhancements.

#### 1.3.1.2 CSP System/Subsystem Design Specification

Author/Source - Informatics General Corporation
Reference Number - TR-85-43232-A004
Date - August 1985/Revised March 1986
Security Classification - UNCLASSIFIED

This document provides a detailed definition of CSP functions and interfaces with other systems and subsystems.

#### 1.3.1.3 CSP Program Maintenance Manual (Volumes I, II, III and IV)

Author/Source - Informatics General Corporation
Reference Number - TR-85-43232-B015
Date - January 1986/Revised March 1986
Security Classification - UNCLASSIFIED

These documents provide detailed program descriptions of all CSP modules and information on the maintenance of these modules. They are technical in nature; designed for personnel responsible for the maintenance of computer programs.

#### 1.3.1.4 CSP Program Specification

Author/Source - Informatics General Corporation
Reference Number - TR-83-43110-13
Security Classification - UNCLASSIFIED

This document describes the program design in sufficient detail to permit program production by the programmer/coder.

#### 1.3.1.5 CSP Configuration Management Plan (CMP)

Author/Source - Informatics General Corporation
Reference Number - TR-85-43232-A009
Date - Revised March 1986
Security Classification - UNCLASSIFIED

This document specifies procedures for the achievement of CUBIC configuration management for the subset of all CSP software developed, disseminated, and/or maintained under the CUBIC Management Program.

#### 1.3.1.6 CSP Software Quality Assurance Program Plan

Author/Source - Informatics General Corporation
Reference Number - TR-85-43232-B017
Date - September 1985/Revised December 1985
Security Classification - UNCLASSIFIED

This document identifies requirements and procedures for CSP software quality assurance.

#### 1.3.1.7 CSP Accreditation/Certification Test Plan and Procedures Manual

Author/Source - Informatics General Corporation
Reference Number - TR-85-43232-A008
Date - August 1985
Security Classification - UNCLASSIFIED

This document is used to plan and conduct tests to satisfy both the AUTODIN Category III requirements of DCAC 370-D195-3, June 29, 1981, and the security and telecommunications accreditation requirements of DoD C5030.58-M for the CSP system in a stand-alone or front-end environment.

#### 1.3.1.8 CSP User's Manual

Author/Source - Informatics General Corporation
Reference Number - TR-86-43232-B007
Date - August 1985/Revised March 1986
Security Classification - UNCLASSIFIED

This manual provides the user's non-ADP communications messages distribution personnel with the information necessary to effectively use the CSP system.

#### 1.3.1.9 CSP Training Course Outline

Author/Source - Informatics General Corporation
Reference Number - TR-85-43232-A012
Date - December 1985/Revised March 1986
Security Classification - UNCLASSIFIED

This outline contains a general slide presentation of the CSP system and a training scenario which attempts to simulate any possible problems which may occur.

#### 1.3.1.10 CSP Training Material

Author/Source - Informatics General Corporation
Reference Number - TR-85-43232-A013
Security Classification - UNCLASSIFIED
Consisting of the following manuals:

General Overview
Date - December 1985/Revised March 1986

For Communication User
Date - December 1985/Revised March 1986

For Computer Operation
Date - December 1985/Revised March 1986

Computer Operation Reference Guide
Date - December 1985/Revised March 1986

**1.3.1.11 CSP Computer Operation Manual**

Author/Source - Informatics General Corporation
Reference Number - TR-85-43232-B014
Date - November 1985
Security Classification - UNCLASSIFIED

**1.3.1.12 CSP Configuration and Installation Guide**

Author/Source - Informatics General Corporation
Reference Number - TR-43232-B000
Date - November 1985
Security Classification - UNCLASSIFIED

**1.3.2 Other Related Documents**

These manuals or documents provide supportive literature concerning the CSP. They may be obtained from the agency or organization indicated.

**1.3.2.1 DCAC 370-D175-1 DCS AUTODIN Interface and Control Criteria (U)**

DCS procedures for the control of data interchange between interconnected elements of DCS AUTODIN.

**1.3.2.2 DCAC 370-D195-3, Test and Evaluation DCA AUTODIN Category III Certification Test (U)**

DCS policy, guidance and procedures for the conduct of Category III certification tests

**1.3.2.3 DoD C5030.58-M, Defense Special Security Criteria and Telecommunications Guidance (C)**

Accreditation criteria for the CSP.

**1.3.2.4 DIAM 50-3, Physical Security Standards for Sensitive Compartmented Information Facilities (U)**

Physical security requirements for facility accreditation.

**1.3.2.5 DIAM 50-4, Security Compartmented Computer Operations (C)**

Guidance and requirements for accreditation of backside ADP systems.

**1.3.2.6 DIA/RSS-4C letter, 15 May 1979; SCI TEMPEST Policy and Guidance on Control of Compromising Emanations (C)**

TEMPEST requirements for SCI facilities.

**1.3.2.7 NACSEM 5100, Compromising Emanations Laboratory Test Standard Electromagnetics (C)**

Engineering criteria and standards for TEMPEST.

**1.3.2.8 JANAP 128, AUTODIN Operating Procedures (U)**

Formats and procedures to be used in preparing and processing GENSER messages.

**1.3.2.9 DSSCS Operating Instruction 102, Routing Indicators (S-CCO)**

RIs, TCCs, etc. for all DSSCS tributaries.

**1.3.2.10 DSSCS Operating Instruction 103, System/Data Procedures (C)**

Formats and procedures to be used in preparing and processing DSSCS messages.

**1.3.2.11 Allied Communications Publication 117, Routing Indicator Book (U)**

GENSER routing indicators for all tributaries.

**1.3.2.12 Allied Communications Publication 127, Communications Instructions - Tape Relay (U)**

General operating procedures for telecommunications centers.

**1.3.2.13 IAS SYSGEN and Startup Guide**

Digital Equipment Corporation, Order AA-2519D-TC.

**1.3.2.14 IAS EXEC Facilities Reference Manual**

Digital Equipment Corporation, Order AA-H005A-TC.

**1.3.2.15 IAS System Management Guide**

Digital Equipment Corporation, Order AA-2520D-TC.

**1.3.2.16 Teleprocessing Line Controller TLC-100-6025 (T) Operation Maintenance Manual**

**1.3.2.17 1562 Dual Monitor Terminal Operator's Manual**

Sperry Univac PX12323 (U).

**1.3.2.18 Delta Data Manuals Related to the 8260T Video Display Terminal**

Delta Data Systems Corporation.

**1.3.2.19 MACRO-11 Reference Manual**

### 1.3.3 CSP Project Sponsor

The CSP project development, distribution and maintenance is under the auspices of AFIS/IND, Bolling Air Force Base, Washington, D.C.

AFIS/IND is the management authority for all CSP activities and, as such, is the single point of contact for further information concerning CSP. Inquiries regarding this manual, or any other aspects of CSP, should be directed to them.

In addition, RADC (Rome Air Development Center), Griffiss Air Force Base, New York, is a join sponsor of the CSP project. RADC is involved in the following areas of CSP: contracting, procurement, technical engineering, security clearance billets, and administrative support for document review.

### 1.3.4 User and Operating Centers

The following is a list of CSP Operating Centers (i.e., users):

AFIS - Bolling AFB, Washington, D.C.
CINCPAC - Camp Smith, HI (USA)
DIA - Washington, D.C.
EUCOM - AIDES - Stuttgart, GE (USA)
FSTC - Charlottesville, VA (USAF)

FTD - Wright-Patterson AFB, OH (USAF)
JSOC - Fort Bragg, NC (USA)
LANTCOM - Norfolk, VA (USA)
MAC - Scott AFB, IL (USAF)
NAVINTCOM - Suitland, MD (USA)
NORAD/SPACECOM - Colorado Springs, CO (USAF)
NOSC - San Diego, CA (USA)
NPIC - Washington, D.C.
REDCOM - MacDill, AFB, FL (USAF)
SAC - Offutt AFB, NE (USAF)
TAC - Langley AFB, VA (USAF)
TCATA - Fort Hood, TX (USA)
TFC - GE (USAF)
TREDS - Metro Tango, GE (USAF)
USAFE COIC - Ramstein AB, GE (USAF)
USAREUR - Heidelberg, GE (USA)
USAFE OSC - Ramstein AB, GE (USAF)
U.S. Treasury - Washington, D.C.

## 1.4 Acronyms and Abbreviations

The following is a list of acronyms and abbreviations used in this document:

ACP Allied Communications Publication
ADP Automatics Data Processing
ADPS Automatic Data Processing System
AFIS Air Force Intelligence Service
AIG Address Indicator Group
Altroute Alternate Message Routing
AMPE Automated Message Process Exchange
AMPSSO AMPE System Security Officier
AN/GYQ-21(V) DoD nomenclature for DEC PDP-11 based systems
ASC AUTODIN Switching Center
ASCII American Standard Code for Information Interchange
ASP Analyst Support Processor
AUTODIN Automatic Digital Network
BAUDOT Code for transmission of date in which five equal-length bits represent one character (BAUD).
BR-1569 Bunker Ramo Multiplexer
BR-1731 Bunker Ramo Multiplexer
$C^3I$ Command, Control; Communications and Intelligence
CARP Contingency Alternate Routing Plan
CDSN Channel Designator and Sequence Number
CIC Content Indicator Code
CID Communications Implementation Directive
CINCPAC Commander-in-Chief Pacific
CM Configuration Management
CMB Configuration Management Board
CMP Configuration Management Plan
CMS Configuration Management System

COMP COMParison every thirty minutes of Mode II AUTODIN line
CPU Central Processing Unit
CRC Cyclical Redundancy Code
CRITICOM Critical Intelligence Communications
CRT Cathode Ray Tube
CSN Channel Sequence Number
CSP Communications Support Processor
CT Communications Technician
CUBIC Common User's Baseline for the Intelligence Community
DAG DSSCS Address Group
DAN Disk Address Group
DCA Defense Communications Agency
DDCMP Digital Data Communications Message Protocol
DDI Delivery Destination Indicator
DEC Digital Equipment Corporation
DECNET Digital Equipment Corporation Network
Delta Data 8260T Viedo Display Terminal
DIA Defense Intelligence Agency
DIAM Defense Intelligence Agency Memorandum
DoD Department of Defense
DoDIIS Department of Defense Intelligence Information Systems
DSAP Data Systems Automation Program
DSSCS Defense Special Security Communications System
DTG Data Time Group
EBDIC Extended Binary Coded Decimal Interchange Code
EOF End of File
EOM End of Message
ETX End of Text
EUCOM European Command
FARM Fully Automated Routing of Messages
FDMP Full Duplex Message Protocol
FSTC Foreign Science and Technology Center
FTD Foreign Technology Division
GENSER General Service
NOSC Naval Ocean Systems Center
NPIC National Photographic Interpretations Center
NSA National Security Agency
NSS NMIC Support System
OCR Optical Character Reader
OISS Operational Intelligence Support System
OJ-389-(V)/G DoD nomenclature for the Sperry-Univac 1652 Dual Scren Terminal
OM Operator's Manual
ORI Originating Routing Indicator
OSRI Originating Station Routing Indicator
PACOM Pacific Command
PAD Pointer and Descriptor
PCL11 Parallel Communications Link (DEC)
PLA Plain Language Addressing

PMM Program Maintenance Manual
QA Quality Assurance
RADAY Radio Day
RADC Rome Air Development Center
RDP Remote Distribution Printer
REDCOM Readiness Command
RI Routing Indicator
RLS Routing Line Segregation
RMS-11 IAS Record Management Services
ROM Read Only Memory
SAC Strategic Air Command
SAO Strategic Activities Office
SI Special Intelligence
SPECAT Special Category
SPINTCOM Special Intelligence Communications
SQA Software Quality Assurance
SSB Standard Software Base
SSN Station Serial Number
SSO Special Security Office
SVC Service Clerk
SVP Service Printer
TAC Tactical Air Command
TCATA TRADOC Combined Arms Test Activity
TCC Telecommunications Center
TEMPEST Control of Compromising Emanations
TFC Tactical Fusion Controller
TLC Telecommunications Line Controller
TOR Time of Receipt
TOT Time of Transmission
TRADOC Training and Doctrine Comm
TREDS Tactical Reconnaissance Exploitation and Demonstration System
USAF United States Air Force
USAFE COIC United States Air Force Europe Combat Operations Intelligence Center
USAREUR United Sates Army Europe
USAFE OSC United States Air Force Europe Operational Support Center
USN United States Navy
USS User Support System
VFK Variable Function Key
ZICON Zone of Interior Comm Network

## SECTION 2. SYSTEM OVERVIEW

This section briefly describes the CSP and the applications for which it is intended.

### 2.1 General Description

CSP can best be described as a collection of application and system level computer programs, designed to execute as a coordinated system, for the express purpose of store and forward operations on record copy message traffic. While there are many ancillary functions of CSP (all of which will be covered subsequently), its primary task consists of reception of message traffic, validation of proper format, determination of required routing, and finally, delivery to the intended recipient.

In and of itself, CSP is merely a message management system. Stripped of all ancillary processing, CSP is a system which reliably moves data from one point to another. It is this ancillary software, however, that defines the characteristics of the data being moved, and what operations are performed along the way.

### 2.2 Applications

By virtue of DCA Category III and DoD 5030-58M guidelines, CSP is accredited to operate as an AMPE system for automation of telecommunications centers. Common examples of CSP environments are Air Force SSO TCCs or Navy SPINTCOM facilities. In its simplest form, CSP serves as an AUTODIN interface for an ASC tributary. Here CSP is responsible for reception, routing, and delivery of incoming traffic, as well as the validation and transmission of outgoing traffic. CSP may also serve in the capacity of a dual home NARC, acting as a relay to other automated or non-automated backside tributaries in addition to serving the local TCC.

### 2.3 Organization

The following paragraphs discuss the organization of CSP with respect to areas of application. Refer to the referenced figures as an aid in visualizing potential installations and applications.

### 2.3.1 Standard System

Common to all CSP installations is the standard system. This is the minimum configuration required to support the CUBIC baseline CSP. Figure 2-1 depicts this baseline system at the organizational level. Automation of the TCC is at a minimal level. While this configuration is possible only in a small communications center, it is important to note that system capability, throughput, etc., is the same as that of the largest possible installation.

Volume and frequency of CSP message traffic is completely site dependent and varies greatly between CSP installations. Current traffic volumes in the range of 2000 to 3000 messages per day appear to be average although several sites have reported fluctuations well above this range. CSP has consistently exhibited the ability to handle large fluctations in message trafic with no sign of system degradation.

The standard system consists of a basic AN/GYQ-21(V) system with the following components: CPU, memory (a minimum of 256 KW), system console, tape drives (as required), two 80 MB disk drives line printer, appropriate communications interfaces, Analytics TLC-100 or equivalent, and one or more Univac 1652 (OJ-389) dual screen and/or Delta Data 8260T terminals. Software for the standard system includes the IAS V3.2 operating system and the CUBIC CSP baseline package. Section 5 provides a complete description of these components.

### 2.3.2 Expanded System

Figures 2-2 through 2-4 detail other feasible configurations for the CSP. Installations have a great deal of flexibility in defining the communications interfaces and functional characteristics of the system supporting them. In most cases, CSP reconfiguration or expansion, using baseline modules, does not require a programming effort. Such modifications are made by altering system tables.

## 2.4 Assumptions and Constraints

Two identified areas which may place constraints on the user are budget limitations and the operational environment. To receive the full benefit of the proposed system, disk should be considered as the media for CSP message storage. Operational environment constraints are in two areas: hardware (processor) constraints, and software (operating system) constraints. The processor places constraints on system processing time (throughput) while the operating

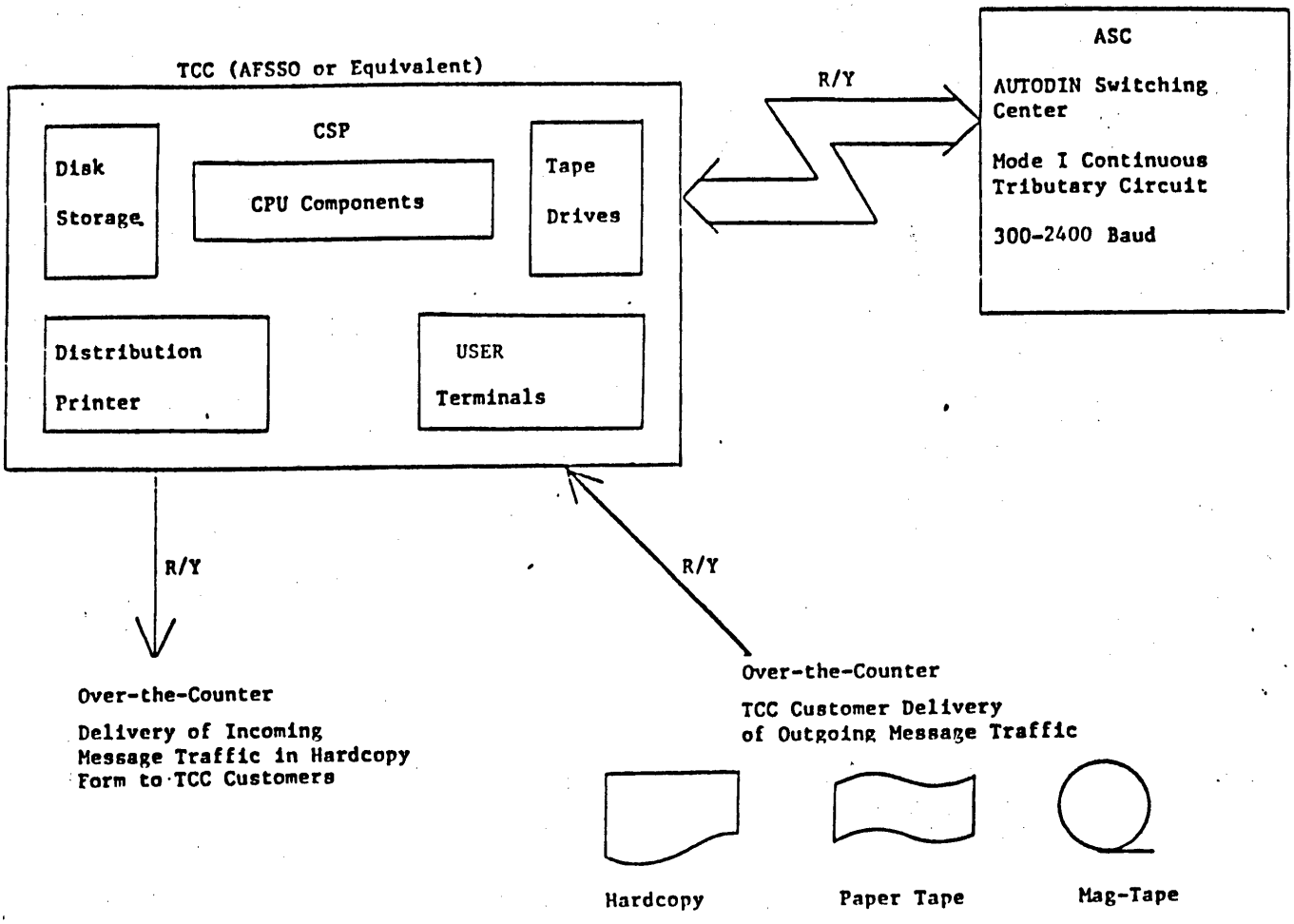


Figure 2-1 CUBIC Baseline CSP

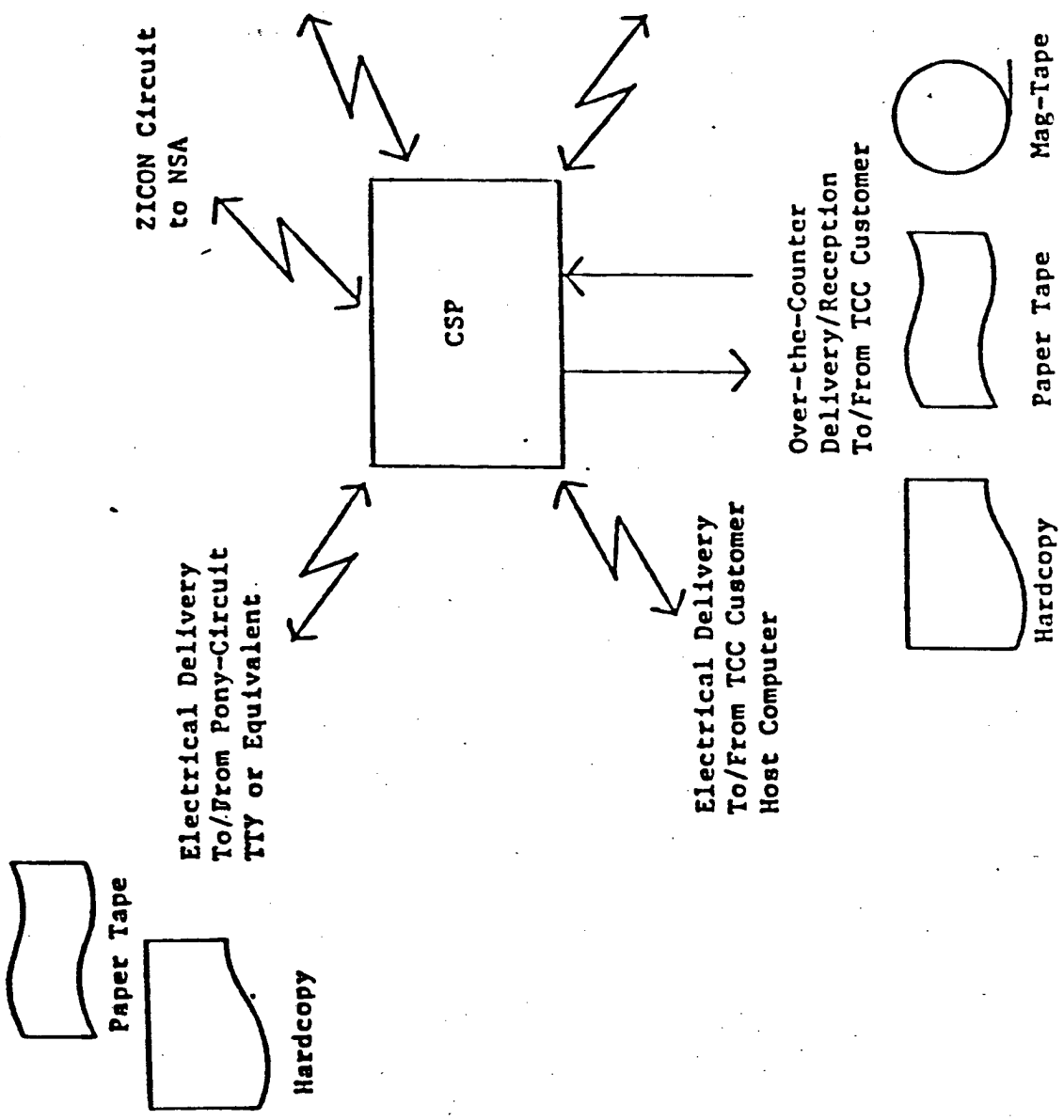


Figure 2-2 Expanded CSP Example 1

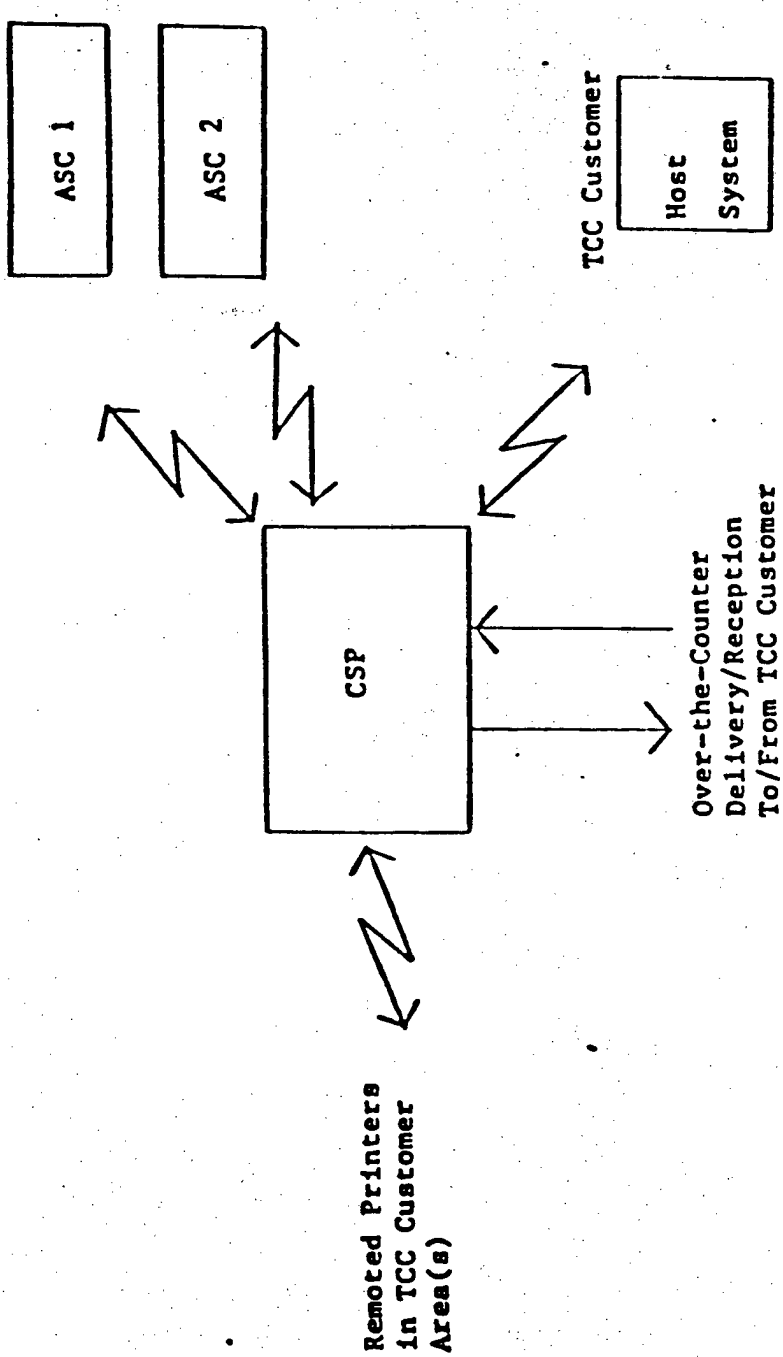


Figure 2-3 Expanded CSP Example 2

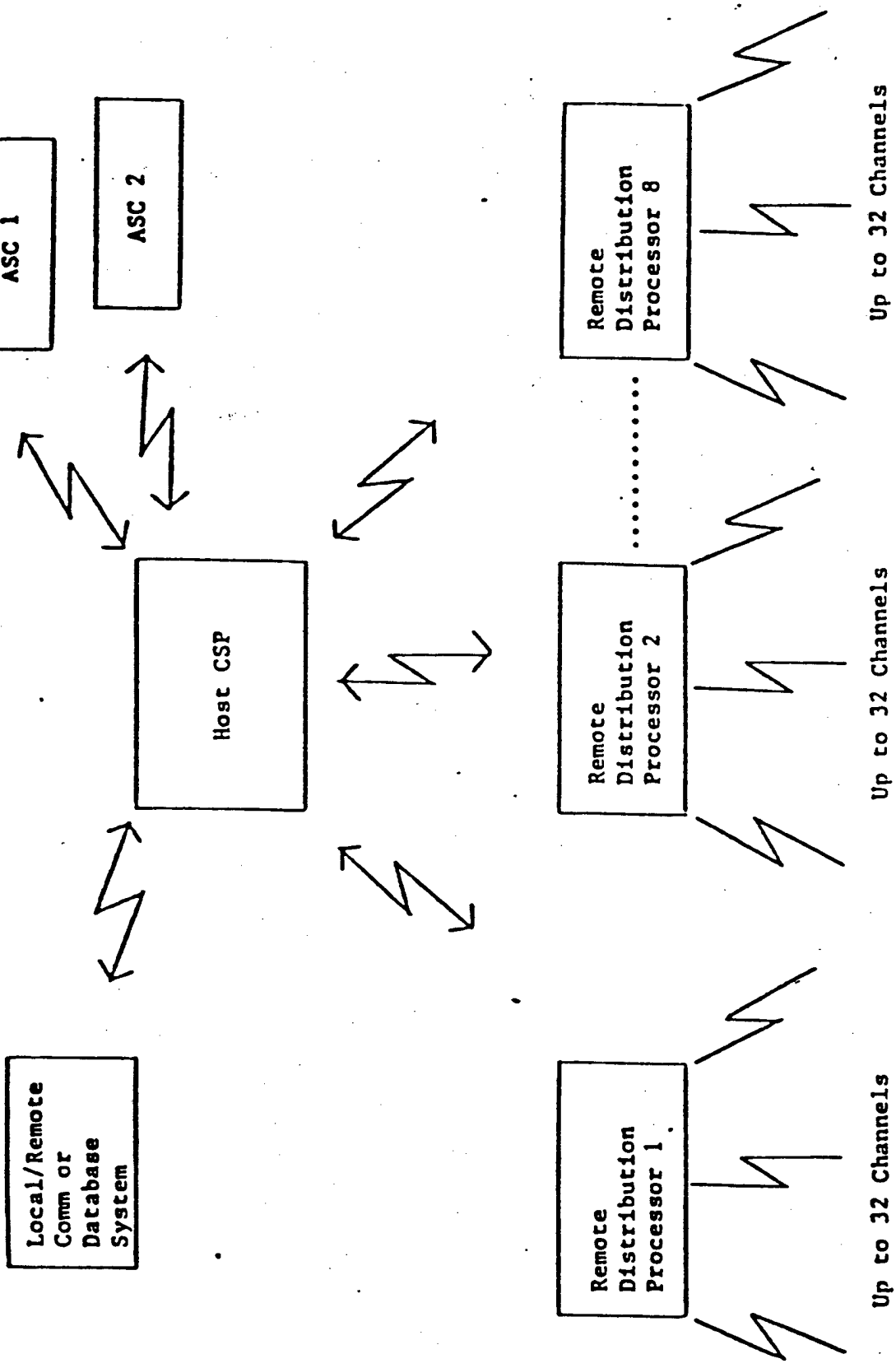


Figure 2-4 Expanded CSP Example 3

system limits the type of communications interface devices which the system may utilize. That is, input/output speed is constrained due to slow interface devices, but the use of advanced communications interface devices is restricted because of the operating system. It should also be noted that the CSP software system is only as secure as the operating system on which it is dependent. In this context, the operating system will place some constraints on total system security.

# SECTION 3. DETAILED CHARACTERISTICS

This section presents a detailed description of each of the operational and functional characteristics of the CSP.

## 3.1 Operational Description

Prior to the discussion of actual system functionality, it is helpful to define the CSP in terms of its users in the operational environment. The following paragraphs describe a typical CSP environment.

### 3.1.1 Definition of Operational Responsibilities

As stated earlier, CSP automates a telecommunications center. Within the TCC there are several functions to be performed, regardless of the mechanisms used. Each TCC must be staffed with at least two persons; a distribution clerk and an administrative clerk. The distribution clerk is responsible for review and dissemination of incoming traffic, as well as the preparation and review of outgoing traffic. The administrative clerk audits traffic and verifies the accuracy and validity of the TCC floor activities (often referred to as Traffic and Analysis). A supervisor must also be available to deal with special case traffic and situations. The supervisor may regularly perform the distribution or administrative clerk functions, eliminating the need for a third person. Operation of the equipment may be accomplished by these personnel, or a separate staff member may be given this responsibility.

These same functions have been incorporated into CSP for purposes of operation and use. There are three main positions defined for CSP operation; each has a general work station. For primary system operation and control, CSP requires a computer operator. This individual is responsible for all aspects of hardware initialization and operation; control of operations such as communication lines; maintenance of system status such as history tapes, system statistics operations, etc.

The second CSP position is the message distribution function. This function is responsible for the review and dissemination of traffic received from AUTODIN, as well as preparing traffic intended for transmission to AUTODIN. Many of the CSP capabilities are primarily directed at facilitating the job of the message distribution function.

The System Supervisor is the third CSP position. While this position is, in some respects, an extension of the message distribution function, the primary function of the system supervisor is to provide CSP with a definition of responsibility for functions which CSP cannot perform automatically or autonomously (such as message deletion). Individuals who properly identify themselves to the CSP as system supervisors are granted certain privileges not available to the message distribution function.

### 3.1.2 Skill Level and Training of User Personnel

The CSP does not require its users to be experienced in data processing concepts or programming, nor does it require experience in computer operations. Persons designated as CSP users are expected to hae training in normal SSO TCC procedures. This usually means persons with Air Force Specialty Codes 291/295 or USN "CT" ratings. These individuals should be fully versed in communications procedures, operation of the equipment normally found in the TCC environment, and the rules and regulations regarding the handling of SI/SAO material.

The CSP user interface is designed with consideration of the training of the 491s and the terminology which has evolved in the TCC environment. CSP is operator friendly; it does not force the user to learn a confusing "data processing" type of language. All commands use a syntax familiar to communicators. Experience has shown that communications personnel adapt to CSP much faster than those with only data processing backgrounds.

### 3.1.3 Accuracy/Validity

The CSP has been designed in strict accordance with accepted quality assurance standards and guidelines. This controlled environment of software design and development ensures that the CSP processes message traffic with extreme accuracy and validity. This is apparent in terms of the proven reliability, integrity, security, and maintainability of the CSP software.

#### 3.1.3.1 Reliability

Several aspects of system operation attest to the reliability of the CSP. Messages are received and transmitted over all communication lines, with full accountability under all traffic loading situations. Under extreme saturation conditions, the input lines are

automatically shut down, in an orderly fashion, while the output lines are allowed to reduce the queued messages within the system.

During the actual processing of a message, each message is subjected to rigorous format validation, which consistently ensures that the format is complete and proper. Any messages found with format errors are rejected by CSP and sent to the designated remote office service position for manual review and correction by the communications supervisor of the remote office.

If unexpected error occur during reception or transmission of messages, due to hardware or line problems, CSP will protect the message it was processing. If transmission was in progress, the entire message will be retransmitted when the problem is corrected. If reception was in progress, the message will not be acknowledged, so the sender will know to retransmit the message.

### 3.1.3.2 Integrity

The CSP system leaves a well established audit trail and maintains strict accountability for all messages processed by the system. This is accomplished by dual recording of each message processing state on the primary message file disk and the redundant device (secondary message file disk and or history tape). Thanks to this mechanism, CSP has never lost a message as a result of software or hardware failure, where proper operator action was taken.

The integrity of the CSP software is apparent in the handling of error (and other unexpected) conditions. Aborted software is a very rare condition.

### 3.1.3.3 Security

The security protection afforded the messages within CSP is achieved through many security practices. As a stand-alone system, the CSP does not prohibit access to the message file by the system manager; but only messages processed by a remote office are available to that remote office. However, it is necessary to enforce, at all levels, strict security procedures on the operation of the CSP.

Prior to the operational acceptance of the CSP, the facility in which it is located must be formally accredited by DIA for a security level commensurate with the highest classification of the information processed by the system. The facility requirements for DIA accreditation are contained in DIAM 50-3 and the appropriate military department security

regulations. DIAM 50-4 contains guidance on accrediting backside ADP systems. Care must be exercised in installing the CSP in the accredited area to minimize the possibility of inadvertent exposure of classified material to uncleared personnel. All printers, system consoles, MDC and SVC terminals, and operator work stations must be placed away from doors and message delivery windows which open into areas of lesser classification. The overall physical configuration of the facility and system will be considered when granting security accreditation to the CSP.

In addition to the facility accreditation described above, the site must be granted a format TEMPEST accreditation by DIA prior to operational acceptance of the CSP. This is to ensure that the hardware installation complies with existing red/black engineering criteria, and the equipment itself does not emanate compromising signals beyond the physical control zone established for the facility.

All personnel who operate the CSP on a daily basis or who are permanently assigned to the facility must be cleared and indoctrinated for all security levels processed by the system. All other personnel, who are not appropriately cleared or indoctrinated but require periodic or one-time access to the facility, must be properly escorted. It is incumbent upon each person assigned to the facility to understand their responsibilities for safeguarding the classified material residing in and produced by the CSP. Final security accreditation is contingent upon strict enforcement of personnel security policies.

This combination of physical, TEMPEST, and personnel security prevents unauthorized access to the CSP. However, an additional level of security is required within the CSP software, to ensure the proper protection of the data within the CSP and to prevent unauthorized transmission of messages over uncleared communication lines.

For each message received or transmitted by the CSP, an input or output security check is performed, ensuring that the particular receive or transmit line is authorized to pass that level of traffic. This is determined by scanning Format Line 12 and extracting all classifications, codewords, caveats, and compartments and comparing them to the codewords, caveats, etc. allowed for the communications line. Any mismatches encountered cause the message to be placed on the supervisor queue, who takes appropriate action. This process allows the accreditation of the CSP for concurrent processing of DSSCS and GENSER messages, since the appropriate level of protection for each is guaranteed.

### 3.1.4 System Usability and Accessibility

CSP is designed with a table-driven architecture. As such, site-unique and remote office unique configurability can be achieved easily by modification of a few key tables defining system lines and queues. All operational system tables including routing indicators, office symbols, user identifications, routing line segregation criteria, and line security parameters are maintained by updating a data file and running an online program. This method provides a simple, reliable, and effective means of updating parameters requiring frequent modifications. From a user's standpoint, therefore, the system configuration can be readily changed without software modification.

## 3.2 Functional Description

The following paragraphs present an itemized summary of CSP functionalities. Many of the functions are optional and are activated as necessitated by user requirements.

### 3.2.1 Communications Interfaces and Characteristics

For the most part, any given CSP installation is unique by virtue of the communications circuits to which it is connected. The distributed baseline system contains a library of interface software modules (referred to as "gateways"), any of which may be selected for configuration. Usually, inclusion of an interface requires only that the circuit equipment be in place and that it have the characteristics indicated below. Individual sites have control over the line names, security level, and routing to any particular line. Detailed configuration information is presented in Section 4 and the CSP Configuration and Installation Guide.

Paragraph 3.2.1.1 describes the AUTODIN Mode I interface and paragraph 3.2.1.2 describes other Mode I interfaces. Each of the Mode I interface descriptions is presented in the following fashion: 1) a general overview of the interface; 2) the protocol (if any) used for actual communiation (e.g., DDCMP, Bisync, AUTODIN, etc.); 3) allowable message formats over the circuit, such as JANAP-128, DOI-103, etc. (see paragraph 3.2.2.2 for a description of supported formats); 4) the message structure which may be handled over the circuit (see paragraph 3.2.2.3 for a description of supported structures); and 5) DoD or other non-CSP documentation of supportive or descriptive information about the interface. Paragraph 3.2.1.3 deals specifically with Mode II circuits. These lines do not have automatic accountability and rely on

human intervention for accuracy and continuity verification. Finally, paragraphs 3.2.1.4 through 3.2.1.9 describe interfaces which are neither Mode I nor Mode II specifically, but for which accuracy and continuity are factors of CSP techniques and hardware capabilities.

The current CSP system is configured to allow a maximum of 64 output queues. Communications lines must be connected to an operating queue to function in the CSP environment. Although system queues such as SVC, MDC, etc., do not utilize communications lines, they do require queues. With the 64 queue limitation, it is still possible to use up all available queues.

### 3.2.1.1 CSP/AUTODIN

AUTODIN is the primary means by which CSP provides access to/from other communications facilities world-wide. AUTODIN consists of a network of switching centers (ASCs) within the United States and overseas which provide multiple-path message traffic delivery between individual DoD communication facilities. There are several levels of interface to a particular ASC and, depending upon the nature of a given facility, more than one ASC.

There are two levels of ASC interfaces, which cover most CSP installations. The first is as a simple tributary circuit. In this case, CSP is connected to one ASC and generally serves as the final destination for message traffic. The second level is a dual-homed non-AUTODIN relay center (NARC). Here, CSP is connected to two ASCs and provides relay services to backside communication centers or host systems. Aside from the physical connections to the ASCs, the only difference with respect to the CSP is in the nature of the routing indicators used; this is a function of proper table set-up (see paragraph 3.2.6.1).

#### 3.2.1.1.1 Protocol

The CSP communicates with an ASC as a Mode I, synchronous tributary in continuous mode. The character set is ASCII and the baud rate may be set from 300 to 2400 buad. The protocol is AUTODIN Mode I as defined in DCAC 370-D175-1. This protocol generally provides for transmission of message traffic in segments of 80 character lineblocks, framed by appropriate control characters.

To alleviate the overhead of blocking/deblocking messages, the CSP relies on a pre-processor, such as the Analytics TLC-100 (or equivalent). This device performs several functions which simplify the interface. The

significant function in this application is blocking/deblocking and conversion from synchronous (to the ASC) to asynchronous (to the CSP). This pre-processor may be connected to the CSP using the BR-1569/1731 or other asynchronous interface devices such as the DEC DV11.

#### 3.2.1.1.2 Message Formats

The AUTODIN interface may be used to transfer the following message formats:

- o DOI-103M (old DOI-100)
- o DOI-103 (narrative and data pattern)
- o JANAP-128 (narrative and data pattern)
- o JANAP single card

#### 3.2.1.1.3 Message Structures

This interface supports only record copy structure. Allowable variations within this structure are indicated by Language Media Format codes (LMFs). By definition, CSP is an ASCII tributary, or NARC. It may receive data from the ASC in either fixed-length record blocks (LMFs A and T) or variable length (LMFD). At this time CSP may transmit only fixed-length record blocks (LMFs A and C).

#### 3.2.1.1.4 References

AUTODIN protocol and message formats are described in paragraph 1.3.2.1.

### 3.2.1.2 CSP/Other Mode I

In addition to AUTODIN, CSP supports a number of other Mode I interfaces; in all cases they are computer-to-computer circuits.

#### 3.2.1.2.1 CSP/Modular Architecture for the Exchange of Intelligence (MAXI)

MAXI is another element in the CUBIC family of computer systems sponsored by AFIS/IND. Its primary purpose is automating intelligence data handling processes within various installations. MAXI is capable of performing the AUTODIN communications functions provided by CSP, but many installations warrant utilization of CSP as a front-end communications processor due to the extent of other non-MAXI traffic handling requirements.

#### 3.2.1.2.1.1 Protocol

CSP communicates with MAXI in much the same fashion as with AUTODIN. The major differences between the MAXI interface and the AUTODIN interface are that MAXI has an asynchronous interface level. This difference eliminates the need for the pre-processor used in the CSP/AUTODIN interface.

The CSP/MAXI interface is implemented via the Western Union PTC port of the BR-1569/1731. AUTODIN Mode I protocol is used and the character set is ASCII. The gateway which interfaces MAXI is a slightly modified version of the AUTODIN gateway; the modifications involve the connect/disconnect protocol between the two systems. All other interface aspects closely follow those of the AUTODIN interface.

#### 3.2.1.2.1.2 Message Formats

The CSP/MAXI interface may be used to transfer the following types of messages:

- DOI-103 (narrative and card)
- JANAP-128 (narrative and card)

#### 3.2.1.2.1.3 Message Structures

CSP and MAXI communicate in record copy structure only.

#### 3.2.1.2.1.4 References

Consult AFIS/IND for technical documentation concerning MAXI. Paragraph 1.3.2.1 provides information concerning AUTODIN protocols, although it cannot be used for specific information concerning this interface.

### 3.2.1.2.2 CSP/Analyst Support Processor (ASP)

The ASP is another type of intelligence data handling system. This system is part of the Strategic Air Command IDHS system and serves a similar function as MAXI. While the ASP is not generally available, the interface to it from the CSP is generic (rather than ASP specific) in nature, thus providing users with an optional interface to another system using this specific protocol.

#### 3.2.1.2.2.1 Protocol

The CSP communicates with the ASP using DDCMP link level protocol. The communication link terminates in a BR-1569/1731 port configured to support the DDCMP discipline. Operation is in synchronous mode using ASCII 8-bit data at up

to 9600 baud. The message protocol is the Full Duplex Message Protocol (FDMP) which controls the flow and accountability of message blocks.

#### 3.2.1.2.2.2 Message Formats

The ASP interface may be used to transfer all CSP supported message formats (see paragraph 3.2.2.2).

#### 3.2.1.2.2.3 Message Structures

This interface supports only record copy structure.

#### 3.2.1.2.2.4 References

ASP documentation may be obtained from the SAC OISS program.

### 3.2.1.2.3 CSP/CSP

The CSP provides an interface which supports message traffic between the CSP and other CSP or CSP-like systems.

#### 3.2.1.2.3.1 Protocol

The interface to other CSP/CSP-like systems uses a synchronous line in a DEC DV11. DDCMP line discipline is used to establish and maintain the logical communication path for controlled transfer of data between the CSP and other CSP/CSP-like systems. Data characters are 7-bit ASCII and may be transmitted/received at line speeds up to 9600 baud.

Transmit/receive operations are controlled separately by the CSP gateway and may be operated independently of each other.

#### 3.2.1.2.3.2 Message Formats

This interface will handle all CSP supported message formats (see paragraph 3.2.2.2).

#### 3.2.1.2.3.3 Message Structures

The CSP communicates with other CSP/CSP-like systems in record copy structure.

#### 3.2.1.2.3.4 References

Information on DDCMP protocol and interface specifications is available from Digital Equipment Corporation in the form of the Digital Data Communications Message Protocol Specification (March 1, 1978).

### 3.2.1.2.4 CSP/IGC

The Message Support System (MSS) implemented at PACOM Data Systems Center at Camp H. M. Smith, Hawaii relies on Intercomputer Communications (IGC) software to provide both interprocessor communications among functional task groups residing in separate physical processors and intraprocessor communications among functional task groups residing in the same physical processor. The CSP/IGC interface requires communications between separate processors.

#### 3.2.1.2.4.1 Protocol

The MSS IGC contains code to support task-to-task protocols, processor-to-processor protocols and code to drive the DEC Parallel Communications Link (PCL11) connecting two processors via a half-duplex data transfer channel. Data may be transferred at rates up to 1000K/second.

#### 3.2.1.2.4.2 Message Formats

The CSP/ICC interface will handle all CSP supported message formats (see paragraph 3.2.2.2).

#### 3.2.1.2.4.3 Message Structures

The CSP communicates with the ICC software via Files-11 structured files. Each message is placed in a single Files-11 file, with or without ancillary information (banner stamps, etc.) and transferred as a whole unit.

#### 3.2.1.2.4.4 References

Information on the PCL11 maya be obtained from Digital Equipment Corporation. ICC interface information may be obtained from PACOM Data Systems Center, Camp H.M. Smith, Hawaii.

### 3.2.1.3 Mode II

CSP interfaces a variety of Mode II communication type devices. Such devices are incapable of acknowledging receipt of message reception, nor can they receive acknowledgement from CSP on message transmission. Additionally, there are

no provisions for automatic error control. Therefore, the verification of continuous and accurate message transfer becomes a critical and rather time consuming function of the operations personnel. Due to the critical nature of this situation, the automatic service message generator was developed. Continuous operation is verified by means of a unique three character Channel Designator associated with a three character Sequence number, assigned and delivered with each message. This, together with a start of message function makes up the first line of the message (often referred to as the "TI" line or Format Line 1), which is transmitted immediately prior to Format Line 2 of each message. With the aid of the automatic service message generator, the "TI" line is scanned for the proper Channel ID/Sequence number. Should an inconsistency be found, the appropriate service message will be built and submitted to CSP for delivery to the appropriate addressee. The operators also visually scan the entire message to ensure accuracy of the data, as no automatic means to do this exists (e.g., block parity, CRC, etc).

For messages received by CSP from a Mode II tributary, CSP verifies the continuity of the Channel Sequence number and identifies inconsistencies in the Channel Designator. Appropriate operator messages are issued under these circumstances and necessary operator controls are provided, as needed, to alter or reset the sequence. For messages transmitted to a Mode II tributary, CSP automatically applies the proper Channel Designator and Sequence number. Again, appropriate operator controls are provided to alter or reset the CSN.

Another feature of CSP, unique to Mode II lines, is the handling of 30 minute COMP messages. These messages are essentially self-addressed test messages generated by a tributary and sent to CSP for the purpose of channel connectivity verification. CSP receives these messages and, depending on their routing, sends them back to the originator, providing verification that the circuit is valid. CSP maintains timers for these messages, on a circuit by circuit basis, and notifies the operator of missing or late COMP messages.

Finally, one of the most important functions of the CSP with respect to Mode II tributaries is the proper acknowledgment of Flash (or higher) messages. Upon receipt of a Flash/Critic/Emergency message from a tributary, CSP responds by transmitting an acknowledgment message to the tributary. If the circuit is receive only, CSP sends the acknowledgment to the system supervisor, but only as an informational notice. For transmission of Flash (or higher)

to a tributary, CSP requires that an acknowlegment message be sent by the tributary within 10 minutes. Non-receipt of this acknowledgment within the prescribed period of time results in operator notification, causing a retransmittal.

#### 3.2.1.3.1 Standard (5-Level BAUDOT)

The Mode II (BAUDOT) communications pseudo handler provides the interface between application tasks (or gateways) and the communications driver (Mode II interface) for Mode II (BAUDOT) lines.

The most common type of Mode II interface for CSP is the 5-level or BUADOT paper tape equipment found in most TCCs. Often this is the Teletype KSR-28; normally this device is interfaced via a BR-1569/1731 multiplexer, using the BAUDOT-CR protocol ROM (Refer to Bunker Ramo Document #MS600-8U11, September 1981).

it can also be interfaced to a DV11 communications driver. These interfaces are able to convert BAUDOT to ASCII to BAUDOT for transmit. They are also able to recognize and cause a software interrupt on receipt of the "EOM" sequence (LF, LF, NNNN).

#### 3.2.1.3.2 NSA (ZICON)

This is a special case of the standard BAUDOT Mode II circuit described above.

For proper operation of a Mode II circuit to NSA (ZICON), a different BR-1569/1731 ROM must be used, specifically the "ZICON" ROM or the BAUDOT-CR ROM. It is modified for ZICON use and known as the SAC BAUDOT-CR ROM. The special characteristics of the ROM deal primarily with the handling of Shift-In (SI) and Shift-Out (SO) characters, to which the NSA equipment is sensitive. Use of something other than the BR-1569/1731 for such an interface can be accomplished with minor software changes.

One other characteristic, pertaining only to an NSA circuit, is the necessity for CSP to recognize and properly time a five-minute line check transmitted by NSA. This check amounts to the CID, CSN of the pre-empted by a normal message. CSP recognizes these pre-emptions and reports non-receipt of a message to the system operator. No further action is required.

#### 3.2.1.3.3 ASCII

CSP is also capable of communicating with ASCII Mode II tributaries. All the characters described above apply, except that the interface device need not perform character conversion, and upon reception must be able to generate a software interrupt on the EOM function, an ASCII ETX, or some other standard end of file function.

Typical interface examples are the use of a Teletype MOD-40 with the BR-1569/1731 ASCII-MOD-40 ROM or, for transmit (from CSP) only, a DEC LA-180 printer driven via DL11 interface. For practical purposes, any device selected for use as a receive (to CSP) device must have paper tape, cassette tape, or floppy disk capability for temporary storage of the complete message, as character-by-character keyboard input of a message (while possible) is extremely difficult to perform accurately and rapidly enough to satisfy CSP timing requirements. This usually precludes use of such terminals as DEC VT-100s, or the equivalent, unless they are equipped as described above.

### 3.2.1.4 Magnetic Tape

The CSP has a limited purpose magnetic tape receive/transmit capability. Its primary purpose is to serve as an alternate method of data transfer between CSP and another system in the event of primary direct electrical link failure, but it certainly can be used for data transfer in other situations. This capability is totally separate from the intercept tape capability (if used) explained elsewhere.

CSP produces magnetic tapes in 9-track, 800 BPI, ASCII, odd parity format, with no labels. Messages are written to tape beginning with Format Line 2 and ending with the normal Format Line 16. Multiple messages may be written to tape with single end-of-file (EOF) marks bet3een messages and a double EOF after all the messages. The record is fixed length, user selectable, and normally 80 characters. Thus the data pattern (LMF "C") messages are evenly blocked on tape and are card image. Narrative messages are also blocked, with full blocks written for all records except the last, which is variable length. End-of-line functions (carriage control) are included.

For receive, much the same applies except that variable-length records may be written (up to 512 characters); and there is no requirement for the single EOF between messages, although it may be present.

Any number of receive/transmit magnetic tape lines may be configured into the CSP (subject to the system capabilities described in Section 5). Normally, regardless of the number of mag-tape sources, only one receive line is required. There should be one transmit line for each different blocking factor required. Also, there should be one transmit line if segregation of traffic (i.e., DSSCS vs. GENSER) is required to separate users.

In the future, CSP will be upgraded to handle variable-length (LMF "D" and "B") magnetic tape formats.

### 3.2.1.5 Paper Tape (8-Level ASCII)

The CSP supports a paper tape reader/punch as an optional feature. Messages are processed via an 8-level paper tape, as well as Mode II BAUDOT paper tape support. A DEC PC11 or an equivalent reader/punch is used.

### 3.2.1.6 Card Reader

Message input via a card reader is supported by the CSP; this is an optional feature. The card reader may also be used for table updates, if the tables are not maintained via disk files. The DEC CR11, or its equivalent, is used.

### 3.2.1.7 Line Printer

The CSP supports three types of line printers: the Message Distribution Printer (MDP), the Service Printer (SVP), and Remote Distribution Printer (RDP). The functions of each line printer are described in the following paragraphs. The functions of the Message Distribution Printer and the Remote Distribution Printer are basically the same, while the Service Printer functions in an entirely different capacity.

#### 3.2.1.7.1 MDP

The Message Distribution Printer prints message traffic according to the standard message distribution format. This includes page numbering (at the top of every page) and classification banner stamping (at the top and bottom of every page). The remote distribution printer processes traffic in much the same manner.

#### 3.2.1.7.2 SVP

Unlike the MDP, the Service Printer does not process pre-formatted messages. Messages with incorrect formats, or some other type of error, can be directed to the Service Printer. The print-outsare then brought to the attention of the Service Supervisor who is responsible for correcting the messages and resubmitting them to the system.

#### 3.2.1.7.3 Remote Distribution Printers

The system has the capability to print message traffic, in Message Distriabution Printer format, at remote printers. This format includes classification banner stamping at the

top and bottom of each page, and page numbers at the top of each page. The systemn provides the optional capability of adding channel designation and sequence numbers to messages printed on a Message Distribution Printer.

### 3.2.1.8 Optical Character Reader (OCR)

The CSP has the capability to interface an OCR, allowing messages to be inputted, without retyping, directly into the system. The OCR scans a typed DD Form 173, prepared by a TCC user, and sends this message to the Plain Language Address elements to communication routing indicators and converts the message to the appropriate format; JANAP 128 or DOI 103.

In addition to this conversion capability, the CSP allows interfacing of a "smart" OCR, which converts to the proper message format in the scanner itself, before the message enters the CSP software.

### 3.2.1.9 Communication User Terminal (OJ-389 or Delta Data)

The CSP provides the communication user with the ability to generate a message at a terminal and subsequently introduce that message into the system. This capability permits generation of fully formatted, as well as DD-173 formatted messages. Additionally, the system provides the optional capability to require message release authorization by the Service Supervisor before allowing transmission to the ASC. The system also allows the optional ability to print messages at either the Service or Message Distribution Printer.

### 3.2.1.10 Message Purge (SCRUB)

The online message file purge capability (SCRUB) gives the CSP System Manager the capability to flag an inactive message to prevent online recall and/or the means to over-write the text of a message to prevent inadvertent disclosure of the text.

### 3.2.1.11 Remote Communications Center

The Remote Communications Center (Remote Office) capability gives the appearance of creating multiple TCCs by breaking the existing TCC, and through the use of multiple user terminals (i.e., OJ-389s or Delta Data 8260s), into two or more separate centers. This allows each TCC to function as a completely separate support entity, without additional hardware/software. This is particularly useful when one TCC is required to support multiple users.

### 3.2.2 Message Processing

Message flow for the CSP (as shown in Figure 3-1) is as follows:

- Message lineblocks are collected and stored on the primary disk and a redundant media (secondary disk and/or magnetic tape) via input gateways. When the complete message is in CSP, the gateway notifies System Control (File Manager).

- File Manager makes necessary records of the new message, and, when satisfied it has positive control, passes acknowledgment back to gateway signifying CSP acceptance of responsibility. The gateway now passes acknowledgment back to the transmitting station (in the case of Mode I). CSP now owns the message.

- The first processing state for all messages regardless of the source is Format Check. The File Manager passes control to the Format Check module.

- Format Check has several validation functions:

  - Message syntax

  - Security categorization, (classification, compartment, codewords, caveats, TCC and LMF).

  - Input security check (to ensure that the input line is authorized to receive a particular security level)

  - Routing (Routing Indicators)

- The next state is output queue determination. File Manager passes control to the Queue Manager which looks at the routing determined by Format Check and queues the message appropriately. If the message has errors (syntax or security), then regardless of where the message was officially routed, it is sent to the service supervisor queue for supervisor action. If no errors are found, the message will be sent to one or more of the following modules:

  - Terminal Operations - user terminal queue (i.e., message distribution or service supervisor) for review and dissemination.

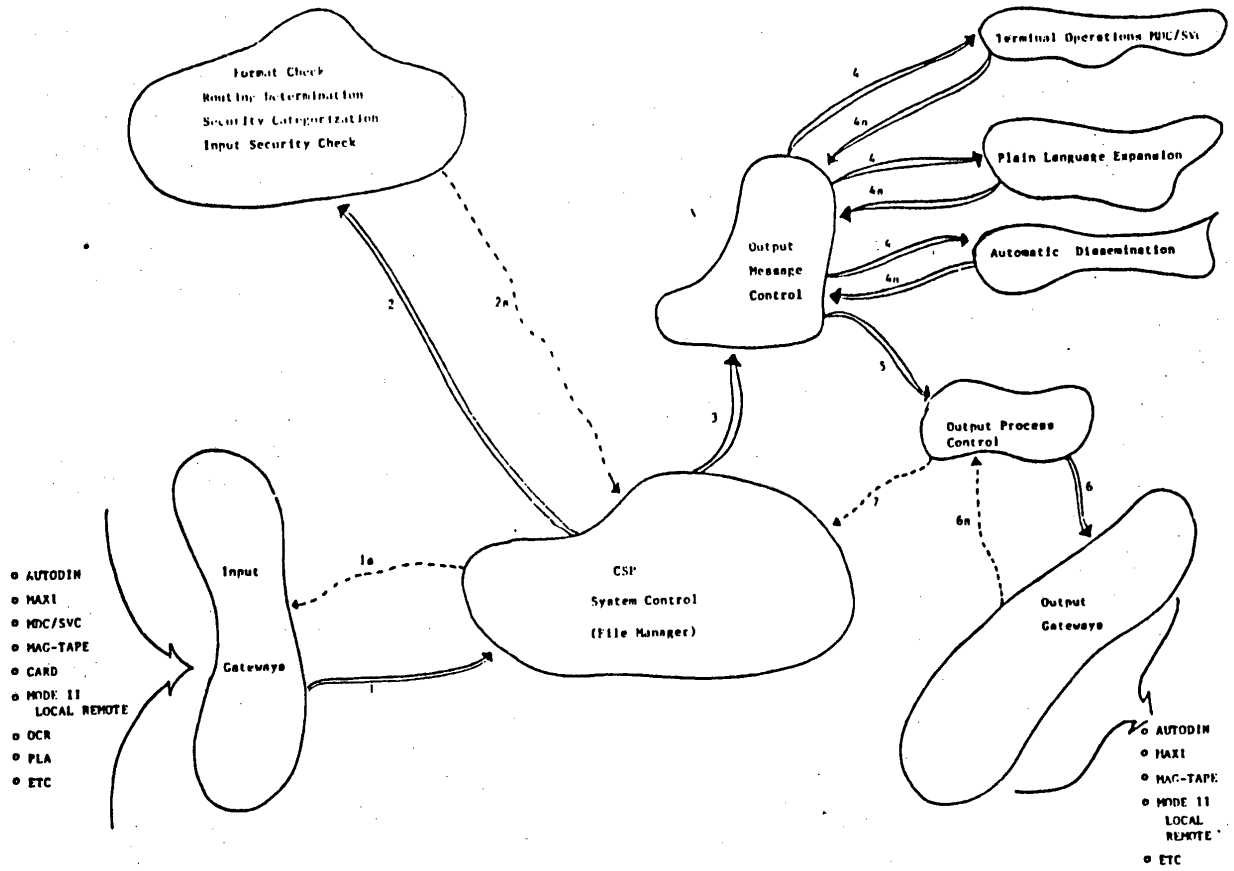


Figure 3-1 CSP Message Flow

- PLA - If the input form of the message was DD173, then the message must be expanded. Note that PLA is a special case here. It has a queue, but PLA is not really an output process. For simplicity, it is treated like an output gateway; but, in fact, PLA will take the message, reformat it, and enter the revised message as a new one.

- Auto-Dissemination - To a large extent, Auto-Dissemination can be viewed as an alternative to Terminal Operations; messages reaching this module are automatically routed and disseminated.

o When these operations are complete, additional dissemination information is stored in the permanent status record and the message is returned to the Queue Manager for further distribution.

o The message now moves to the output process control state where it awaits transmission. Note that the message may be sent directly to output process control from Format Check if the message is derivatively routed.

o As the appropriate transmission line becomes available, the Queue Manager passes the message to the output gateway, which has three major responsibilities:

- Performs an output security check to ensure that the line is cleared for the message.

- Performs routing line segregation to strip routing indicators from the messages which do not apply to this particular line.

- Transmits the message.

o Following successful transmission and receipt of acknowledgment from the receiving station, the gateway passes the acknowledgment status back to the Queue Manager, which updates the permanent status record to reflect successful transmission.

o When the message is successfully sent to all intended addressees, the Queue Manager returns control to the File Manager,which marks the message inactive.

The following paragraphs describe significant components of this process in detail.

### 3.2.2.1 Storage Techniques

CSP utilizes two different recording media in order to accomplish message storage, disk and/or magnetic tape. While disk storage is straight forward, tape storage can take one of three possible forms.

The dual disk capability provides the CSP user with the option of utilizing a second disk (dual disk) as a redundant message recording media. Redundant message recording can be accomplished through the use of a second disk (dual disk) only, history tape only, or via dual disk and history tape. The dual disk redundant message recording capability will greatly improve the speed of all storage media reads and writes.

#### 3.2.2.1.1 Disk

CSP message storage uses a primary message file disk and optionally a secondary disk for redundant recording.

Messages stored on disk are stored in a message file which conforms to Files-11 format for disk I/O operations. The size of the message file is directly contingent upon the amount of free space on the primary disk. For example, with 20,000 blocks of free space on the primary disk, a message file up to 20,000 blocks in length may be created on both disks.

##### 3.2.2.1.1.1 Primary Disk

The primary message file disk must be utilized for CSP operations. All message traffic and processing status information is recorded in the message file. The primary disk can also be utilized as the intercept device in place of tape.

##### 3.2.2.1.1.2 Secondary Disk (Optional)

The secondary disk optionally contains the redundant message file which will be a morror image of the primary disk message file and function in the same manner of recording and updating message traffic and record data. If a secondary disk message file is used, it can be the only redundant media or can be used in conjunction with the history tape.

#### 3.2.2.1.2 Tape

Tape storage can occur in one of three fashions; history, intercept, and output magnetic (mag) tape. All three types store messages in ASCII format, at a density of 800 BPI. History and intercept tapes are blocked at 512 bytes per block, while output mag-tapes are unblocked. History tapes are labeled; output mag-tape is not labeled; and intercept tape may either be labeled or not labeled. Messages on output magnetic and intercept tapes are separated by a file marker between each message. On all three types of tape, two consecutive file markers indicate the end of the tape.

### 3.2.2.2 Message Formats

Seven types of message formats are authorized. The particular format is determined by Format Line 2 of the message.

#### 3.2.2.2.1 DOI-103 and DOI-103C

Message formats for the DOI-103 (narrative) and the DOI-103C (card) differ in several ways. The most notable difference is that two carriage returns and one line feed are found at the end of every line of the DOI-103 (narrative) format; this does not occur in the card format. The following paragraphs describe the formats of DOI-103 and DOI-103C, noting any differnces.

If the message is "piloted", Format Line 1 contains "pilot" information. The pilot information appears as the first line of the message and may contain lines with formats similar to Format Lines 2, 4, and 4a. Since piloted data takes precedence over non-piloted data, the data in succeeding Format Lines 2, 4, and 4a is ignored if a pilot line of that format has already been processed. These lines will, however, be validated for the proper format.

If the pilot is for a suspected duplicate message, character positions 5-8 of the first line of the pilot (the Format Line 2 pilot line) contain the characters "KZFDY". In this case, character positions 29-33, rather than containing the security ("-") and the four-character security field (as in a normal Format Line 2), will contain a space and four alpha characters. The security sentinel and security field then follow immediately, in character positions 34-38.

For other types of pilots, the first pilot line is identical in format to Format Line 2. As stated above, other pilot lines duplicating the formats of Format Lines 4 and 4a

may follow the first pilot lines. If present, the Format Line 4 pilot line contains (in character positions 10-13) a space, followed by a three-letter code starting with "Z". These are accounted for in Format Check.

If a Format Line 4 pilot line is present, characters 7-9 of this pilot "ZNY" line (which constitute a TCC) are saved for comparison with the TCC in the succeeding Format Line 4. If the TCCs do not match, an error condition is noted.

Except for the considerations described above, individual pilot lines are handled exactly as the Format Lines described below.

The remaining Format Lines are verified in accordance with the guidelines found in DOI-103. Individual Format Lines are fully defined in that manual. The only variation of this format is that CSP requires Format Line 12 to immediately follow Format Line 11. The CSP requries Format Lines 2, 4, 11, 15 and 16 to be present and letter perfect. Format Lines 4a and 5 are required to be letter perfect, if they are present. Format Lines 6 and 7 are processed, if recognized, but are not required to be letter perfect.

**3.2.2.2.2 DOI-103M**

If the message is "piloted", Format Line 1 may contain "pilot" information. The pilot information will appear as the first message line and may contain lines duplicating Format Lines 2, 3, 4, and 4a. Since piloted data takes precedence over non-piloted data, the data in Format Lines 2, 3, 4, and 4a is ignored if a pilot line of that format has already been processed.

In all cases, characters 7 through 9 of any pilot "ZNY" line (constituting a TCC) are saved for comparison with the TCC in the succeeding Format Line 4. If the TCCs do not match, an error condition is noted. Aside from the above considerations, the individual pilot lines are handled exactly as their counterparts.

The remaining Format Lines are verified in accordance with the guidelines found in DOI-103. Individual Format Lines are fully defined in that manual. The only variation of this format is that CSP requires Format Line 12 to immediately follow Format Line 11. The CSP requires Format Linesw 2, 3, 4, 11, 15 and 16 to be present and letter perfect. Format Lines 4a and 5 are required to be letter perfect, if they are present. Format Lines 6 and 7 are processed, if recognized, but are not required to be letter perfect.

### 3.2.2.2.3 JANAP-128 and JANAP-128C

Message foramts for JANAP-128 (narrative) and JANAP-128C (card) differ in several ways. The most notable difference is that the two carriage returns and line feed found at the end of every line of the NANAP-128 (narrative) format do not occur in the card format. The following paragraphs describe the formats of JANAP-128 and JANAP-128C, noting the differences.

If the message is "piloted", Format Line 1 may contain "pilot" information. In this case, the pilot information appears as the first line of the message. The pilot may contain lines duplicating Format Line 2. Since piloted data takes precedence over non-piloted data, the data in Format Line 2 will be ignored if a pilot line of that format has already been processed. These lines will, however, still be checked for the proper format.

If the pilot line is present in JANAP-128, the character positions 5 through 8 of this line contain the four character content indicator code (CIC). In both formats, character positions 29 through 33, rather than containing the security sentinel ("=") and the four character security field, contain a space and four alpha characters. The security sentinel and the security field follow in character positions 34-38.

Except for the considerations just mentioned, the pilot line is handled exactly as its counterpart, Format Line 2.

The remaining Format Lines are verified in accordance with the guidelines found in JANAP-128. Individual Format Lines are fully defined in that manual. The only variation of this format is that CSP requires Format Line 12 to immediately follow Format Line 11. The CSP requires Foramt Lines 2, 4, 11, 15 and 16 to be present and letter perfect. Format Line 5 is required ato be letter perfect, if present. Format Lines 6 and 7 are processed if recognized, but are not required to be letter perfect.

### 3.2.2.2.4 JANAP Single Card

The format of the JANAP single card message is fully defined in JANAP-128.

### 3.2.2.2.5 ACP-127

ACP-127 ia a single message format. It will be used to send GENSER messages. This format will be used to transfer messages over a tape relay in narrative form. The format

lines of an ACP-127 message will be verified according to the guidelines found in the ACP-127 manual. Individual format lines are defined in that manual.

#### 3.2.2.2.6 DD-173

DD-173 formatted messages should be prepared in accordance with standard DD-173 message preparation procedures. CSP requires the inclusion of "QQQQ" on a separate line following the classification line to indicate termination of security information. An end of message sequence, "NNNN", is also required by CSP to designate completion of message input. The end of message (EOM) sequence may be typed on the message form by the preparer or may be appended by the CSP operator at the time of transmission.

### 3.2.2.3 Message Structure

The CSP message structures define and limit the interface mechanisms for CSP. A backside interface wishing to communicate with CSP must do so either in straight record communications format or by Files-11 transfer. The following paragraphs describe these methods of message manipulation.

#### 3.2.2.3.1 Straight Record Communication

The most common fashion in which CSP communicates with external interfaces (AUTODIN, backside tributaries, etc.) is in record communications format. The CSP transfers messages on a lineblock by lineblock basis. The message, whole or otherwise, is neither stored in a temporary file, nor is it enveloped in "CSP-added" information (such as banner stamps, distribution markings, audit trail) prior to or during transfer. The first transferred information concerning a given message is Format Line 2 (or Fpormat Line 1 in the case of Mode II). The last transferred information concerning a given message is the EOM sequence (Format Line 16); no other information is transferred, except for protocol information such as control characters, checksum characters, etc. which are necessary for communications link establishment and maintenance.

#### 3.2.2.3.2 Files-11 Structures Files

The second technique by which CSP transfers message traffic is via DEC Files-11 structures files. A message,in its entirety, is placed in a single Files-11 file, with or without ancillary information (banner stamps, etc.) and transferred as a whole unit by whatever means selected for file transfer (DECNET, mag-tape, ICC, etc.).

### 3.2.2.4 Format and Structure Validation

All messages entering the CSP system are checked for proper formatting and consistnecy of message integrity.

#### 3.2.2.4.1 Input

Proper format and structure of the message are ensured by testing and comparing each Format Line within the message against tables and predefined values. Message consistency is determined by comparison of Format Lines to each other.

#### 3.2.2.4.2 Output

Any message found with a descrepancy is flagged with the proper error message, sent to the supervisor review queue for correction, and re-entered into the system. After a message has passed format validation, it is assigned to the appropriate queue.

### 3.2.2.5 Routing and Distribution

CSP routing and distribution mechansims are described in the following paragraphs.

#### 3.2.2.5.1 Routing Indicator Based

The originating station has the responsibility for selecting Routing Indicators for the communication facility serving the addressee.

In determining message distribution, a scan is done of the Routing Indicators contained in Format Line 2 of the message. The Routing Indicators found are checked against a system table for routing assignments. The CSP system can handle several types of routing indicators; each is described below.

##### 3.2.2.5.1.1 Local

Routing and distribution of a message is determined by the Routing Indicators located in Format Line 2. The first four characters of a GENSER message and the first six of a DSSCS message indicate which communication facility receives the message. When the CSP system receives a message, verification is made to ensure the destination is correct. If the message is misrouted, proper action is taken.

#### 3.2.2.5.1.2 Derivative

Derivative distribution is a way for the CSP to further process the Routing Indicators. A system table is defined with respect to the derivative Routing Indicators. As a match is found, the message is routed to the appropriate queue.

#### 3.2.2.5.1.3 CARP

The Contingency Alternate Routing Program (CARP) provides automatic alternate routng of a message. This capability is very useful in the event of system failure or to alleviate backlogs of traffic.

#### 3.2.2.5.1.4 Collective

Collective Routing Indicators allow the operator to route a message to a group of addressees using only one specified Routing Indicator. Single Routing Indicators may be used in conjunction with collective indicators.

### 3.2.2.6 Classification/Security Categorization

Categorization of traffic ensures the proper handling of messages. Through the use of the security tables, the system can identify the classification/security of the message. Processing the traffic through the security tables categorizes the message based on classification, transmission control codes, caveats, and compartments. This makes it possible to check the message security level against the security level of any given communication line.

### 3.2.2.7 PLA Expansion

The Plain Language Addressing (PLA) function allows messages submitted in DD 173 format to be processed as regular narrative traffic. This is done by actually creating a new message in either DSSCS or GENSER format from the one submitted in OCR format. The CSP message file is used to store both the DD 173 message and the new narrative form after conversion.

Prior to converting the DD 173 message to narrative format, each header line in the DD 173 is validated to ensure that an entire message has been received, all the pages have been received in order, and all the required fields contain appropriate data.

Conversion operations consist of validation, expansion, and copying activities. Each field in the DD 173 header line is translated into the appropriate format for a narrative message. Plain Language Addresses on the DD 173 are replaced in the narrative message by Routing Indicators (RIs) obtained from a table lookup operation. An unlimited number of PLAs are supported, each of which may contain over 200 characters. Address Indicator Groups (AIGs) and DSSCS Address Groups (DAGs) are assigned Routing Indicators in a similar fashion, with special provisions made for exemptions. GENSER messages are paged and sectioned when necessary.

Any errors, discovered during the validation and expansion process cause the DD 173 to be routed to the SVC for operator action. Once all PLA processing has been successfully completed, the expanded message is returned to the File Manager which processes it as a new message, using standard CSP procedures.

### 3.2.3 TCC Automation

This section details CSP functionality in areas directly facilitating TCC operations. These functions cover operations which, prior to a CSP installation, are of a manual nature or could be considered operator aids. Items addressed in this section apply primarily to the Message Distribution Position and System Supervisor positions of the CSP (see paragraph 3.1.1).

#### 3.2.3.1 Message Distribution Position Support

There are four major tasks performed by the Message Distribution Position on CSP: message review, message dissemination, message generation, and message recall. Related CSP functions are discussed below.

##### 3.2.3.1.1 Message Review

In most installations, the majority of traffic received byt CSP from AUTODIN requires some level of operator review, primarily for the purpose of dissemination determination. Each site has developed criteria covering how dissemination is to be done. While the criteria may differ for each site, the basic operator funciton is the same; a visual scan of the message is made to identify key fields used for dissemination.

CSP supports this function by providing one or more CRT terminals and terminal-related functions, which allow an Message Distribution Position operator to selectively review

messages requiring dissemination, page forward or backward through a message, and determine the criteria upon which to base dissemination.

These messages are maintained on a priority-ordered queue, allowing the Message Distribution Position to review and disseminate the highest priority traffic first, deferring lower priority traffic until later. If a message with Flash (or higher) precedence is placed on the queue while review of a lower priority message is in progress, the operator is notified via an (audible and visual) alarm. The alarm is cleared and the highest priority message reviewede. Once done, the Message Distribution Position returns to the lower priority traffic. Further aspects of the review function are discussed in the following paragraphs to the extent that review is involved in subsequent Message Distribution Position activities.

### 3.2.3.1.2 Dissemination Via Office Symbols

Message review is the first step in message delivery to the intended addressee. The next step, dissemination, is generally performed during the review process. There are two procedures by which the Message Distribution Position operator may effect dissemination. The first is semi-automatic, while the second is entirely manual. Both may be used interchangeably, depending on operator preference.

#### 3.2.3.1.2.1 Fully Automated Routing of Messages (FARM)

Fully Automated Routing of Messages (FARM) automates the Message Distribution Clerk function. For selected messages, FARM will scan the message heading and the first ten lines of text. Key message elements (classification, codewords, caveats, precedence, privacy/passing instructions, OP signals, O signals, pilots, content indicator code, addressees, DDIs, subject and keywords/phrases in the first 10 lines of text) are then compared against a set of data base tables and a set of office symbols are assigned for delivery. The data base tables specify both the intended and allowed recipients of the message according to site requirements. After recipient office codes have been selected, system data structures are updated in the same manner as for manually selected routing. The message is then placed in the system output queues corresponding to the recipients and delivered automatically.

#### 3.2.3.1.2.2 Light Pen

To allow operators complete manual control of the message dissemination function, CSP provides two related capabilities. Using the features of the dual screen Univac 1652 (OJ-389 or Delta Data 8260T) terminal described in Section 5, the operator is presented with a menu of all the disseminees served by the TCC faciliuty. During message review, disseminees are selected by using the light pen (OJ-389) to touch the CRT on or near the required disseminee symbol or highlighting the required disseminee symbol (8260T). The CSP will then assign the disseminee to the message. Copy count information is appended, but may be modified as needed. If selected in error, previously assigned diseminees may be removed.

The menu may be updated at any time during system operation. In the event that the menu is not current, (i.e., a new disseminee has been identified) operators may manually type the undefined disseminee symbol and copy count into the terminal command buffer; CSP will then transfer it to the current message.

#### 3.2.3.1.3 Message Generation

Outgoing messages are prepared on the MDC terminal using standard text entry and editing features of the terminal. Operators have the option of preparing messages from scratch or selecting oine of several pre-formatted message skeletons and filling in the required fields. After preparation and prior to transmission, the message is reviewed and corrected. Transmission effected aby VFK depression and the message is subjected to format checking, security validation, etc.; and then, as an option, it is queued to the sytem supervisor position for release authorization. This provides complete control over preparation and transmission of outgoing traffic.

Messages prepared on the temrinal may either be fully formatted (in narrative or data pattern) or in DD-173 format. In the latter case, the message is subjected to PLA expansion (see paragraph 3.2.2.7) and queued to the SVC for release authorization.

#### 3.2.3.1.4 Message Recall

Users can also perform message recall functions from their terminals; the recalled traffic is either returned to the terminal for subsequent processing or retransmitted. Specific recall capabilities are detailed in paragraph 3.2.3.6.

### 3.2.3.2 Service Supervisor Support

The system provides additional capabilities to the Service Supervisor. Appropriate validation is performed to ensure that only users with Service Supervisor privileges can perform the following functions: message editing, message deletion and message release authorization/verification.

#### 3.2.3.2.1 Message Editing

The Service Supervisor has the capability to edit an existing message and reintroduce it into the system as a new message. The editing functions include, but are not limited to: line deletion, character deletion, word deletion, character modifications, and new line insertion. The system provides the optional capability to print the edited message on the Service or Message Distribution Printer.

#### 3.2.3.2.2 Message Deletion

The Service Supervisor has the capability to delete a message from the service queue. An audit trail capability is provided; it includes the user's intials and time of deletion. The system provides an optional capability to print the deleted message on the Service or Message Distribution Printer.

#### 3.2.3.2.3 Message Release Verification/Authorization

One of the Service Supervisor's responsibilities is to review certain messages prior to their transmission to AUTODIN. This capability applies to all messages received over input line flagged as requiring release authorization. An audit trail capability is provided, consisting of the user's initial and time of authorization.

### 3.2.3.3 Classification and Security Stamping

When a message is processed, the security tables are searched for the appropriate classification, caveats, codewords, and compartments. As the classification items are found, the appropriate information in the PAD record of the message is set. If hard copies of the message traffic are provided via local or remote distribution printers, the classification information for each message is contained in the message PAD record. The gateway, handling the printers, accesses this information andproduces a classification banner on the top and bottom of each message page. The class stamping capability replaces manual procedures, which are extremely time consuming.

### 3.2.3.4 Message Intercept

The ability to hold traffic for periods of time for subsequent processing provides operator flexibility in running the TCC. There are many situations in which an operator may decide to defer processing until a later time; CSP provides the tools for such deferred processing. CSP is a store-and-forward system and geared for real-time distribution of traffic; however, it is inefficient to keep large amounts of traffic active in the system for long periods of time. Aside from using dynamic system resources, a system failure rendering the online message file unusable at the time of high utility increases the users workload in recovering traffic from backup sources.

The intercept function of CSP provides a convenient method for fast, temporary offline storage of message traffic which, for several reasons, is not immediately processed by the system. The intercept function also acts to drain the system of active traffic, in the event of scheduled or unscheduled shutdowns. Traffic destined for one or more particular tributaries may be alternatively routed to the intercept device (disk or tape) and held until such time as reintroduction to the CSP is desired. This action might be taken in the event a backside host system is down for a period of time and the user does not wish to hold the traffic active, tying up system resources.

Traffic altrouted from a particular output tributary queue(s) to the intercept device (disk or tape) returns to the original queue(s) upon reintroduction into the system.

Message retrieval from the intercept device is possible by selecting a block of messages, selecting by precedence, or selecting by the queue to which the message was originally routed. For example, a user may retrieve all FLASH precedence traffic which was originally routed to the SVC queue.

The intercept tape itself has a special format, intended for use solely by CSP. Sites requiring mag-tape level communication should look at the general-purpose magnetic tape capability rather than intercept, as significant security-related problems arise when attempting to use intercept as a means of external communication.

The actual process of intercepting traffic is straight forward. The desired queues are altrouted to the intercept queue, and the line is turned on. Traffic currently on queue and all subsequent traffic placed on any of the altrouted

queues is transferred to the intercept device. This condition remains in force until it is suspended by the system operator. When the intercept device is closed, a summary log is made detailing what traffic was placed on the device. For re-introduction, the operator suspends the altroutes and turns the recieve intercept line on, specifying that one or more of the messages on intercept device is to be read in. Messages may be read in one by one, in groups, or by the entire file/tape.

Intercepting is also useful in "draining" the system when preparing for a shutdown, in system swap or to replace the message file disk if, for some reason, it is suspected to be unreliable. In this case, the intercept serves as a fast technique for protecting active traffic.

### 3.2.3.5 Alternate Routing of Messages

The CSP operator can redirect message traffic from one output queue to another. This is necessary if circuit outages and hardware difficulties cause device unavailability; it also allows for downloading of all (or selected) traffic to the intercept queue prior to a system shutdown. Not all CSP queues are allowed altroute privileges; there are a specified subset of queues to which an authorized queue may be altrouted. This order is specified and controlled by a CSP system table. Once effected, traffic continues to be redirected until the altroute action is negated by a suspend altroute activity for the queue involved. A system shutdown followed aby a cold start also negates altroute assignments. However, altroute assignments remain in effect if a normal system shutdown is followed by a restart.

### 3.2.3.6 Message Retrievability (Recall)

CSP provides message recall capability from CSP-formatted disk files (online) or CSP-formatted hsitory devices, disk or tape (offline).

The online operation is limited to retrieval of CSP messages still existing on the CSP primary disk message file, allowing fast message retrieval. An added features of this operation is the capability to recall CSP messages, in an offline mode, from an offline CSP-formatted disk file.

The history tape (offline) operation recalls CSP messages from any number of CSP-formatted history tapes, allowing the recall of messages no longer existing in the CSP message file.

### 3.2.3.6.1 Online (Disk)

A message is not recallable if it is currently active, identified as a busted message, or identified as the recalled copy of a CSP message. The following guidelines are used for online (disk) recalls. If the recall is from the system console or the super service position, error-free messages may be recalled. For remote offices, a message may be recalled if the OSRI or one of the format line 2 routing indicators is associated with the office. For all recalls, a message may be sent to the default recall queue, any allowable recall queue specified in the office table, or any queue that the message has been to before. These constraints help maintain CSP file integrity and prevent message duplication within the active CSP file. Messages selected for recall are routed to the remote office default queue or any queue identified in the queue table as valid for recall purposes, assuming it is one of the queues identified in the original message distribution (i.e., a message cannot be recalled if it was not originally routed to the requesting remote office). CSP messages with format errors are considered for recall only if distribution is to the service supervisor, SVP, or system default queue.

The result of an online recall varies, depending on the type of recall search requested. A global data field is established at each CSP operational site. The value contained therein represents the maximum number of messages which any single recall request is allowed. Ths constraint, which can be changed at any time to suit operational needs, prevents an overflow of recalled messages due to erroneously constructed, but syntactically correct, recall requests.

Some ancillary capabilities, which do not recall CSP messages but provide meaningful data and capabilities, include:

- Display of the MLN, DAN, and time-of-receipt from the oldest retrievable message in the primary CSP message file.
- Cancellation of a recall-in-progress at the inputting terminal.
- Aborting of all recalls from all terminals from the system console.

- Provision of a hardcopy of PAD record data fields (from the primary message file) of a specific message. This capability is provided only in conjunction with an MLN or DAN-type of recall request.

### 3.2.3.6.2 Offline (History Device (Disk or Tape))

Offline recall prompts the operator for recall request parameters and identification of hte history device; validates all input; displays an error message and new prompt if input errors are encountered; and once satisfied with the input, proceeds through one or more parameters. The total number of messages selected for recall is displayed to the operator, followed by a display of each message ledger number. The operator determines if the output should be directed to the service printer or to an intercept device for reintroduction into the CSP online system. A maximum of 200 messages can be selected as the result of any single recall request.

### 3.2.3.6.3 Parameters

The online and offline recall systems have different requirements and capabilities. The nature of these requirements/capabilities, the environment (online/offline), and the specific needs of each system dictate the system parameter applicability. Exception parameters, i.e., those parameters only applicable to one of the two systems, are annotated as follows: (online = *); (offline = **). A recall request consists of the search type, search values, and identification of the output queue (*), where the recalled messages are directed.

Search tuypes include: MLN (Message Ledger Number); CDSN (channel Designator Sequence Number); OSRI (Originating Station Routing Indicator); DTG (* Date Time Group); TOT (* Time of Transmission); TOR (** Time or Receipt); and DAN (* Disk Address Number).

Search value inputs vary depending on the search type; the input values identify, if the request is intended to recall a single message, a range of messages or a group (**) of messages.

### 3.2.3.7 Miscellaneous

The following paragraphs discuss several minor features of CSP which assist TCC users in the performance of their duties.

#### 3.2.3.7.1 Come-Back Copy

As an option, any input communications line to CSP (except AUTODIN and NSA) may be configured to specify that a "come-back" copy be returned to it or another circuit in the system. This is particularly useful in the case of Mode II "pony circuits" to/from remote centers which need confirmation of receipt as well as copy of outgoing traffic. This feature works in a similar fashion as "self-addressing", but it obviates the need for actual tributary self-addressing.

#### 3.2.3.7.2 Routing Line Segregation (RLS)

In keeping with standard communication procedures, CSP provides for routing indicator segregation on all transmit communication lines. RLS has several uses within CSP, but its primary function is to strip Routing Indicators not pertaining to a particular communication circuit prior to delivery to that circuit. This ensures that the recipient is not made aware of the Routing Indicators assigned to other addressees.

A secondary use of RLS is to strip local Routing Indicators from a message being reintroduced to AUTODIN. This prevents self-addressed traffic from being sent to the switching center (ASC). In case of alternate routing of traffic to a intercept device, it is also the function of the RLS (by virtue of replacing all RIs on a message with a RI unique to the particular circuit in altroute) to allow such traffic to return to its intended queue when reintroduced.

RLS is completely table driven; the system manager directly sets up and controls the segregation function. By proper use of the table function commands, the user has a large number of options as to how the message traffic is routed within the system and how the segregation function itself is performed. Paragraph 3.2.6 discusses table maintenance for RLS in greater detail.

### 3.2.4 Statistics and Accountability

The following paragraphs deal with the ability of the CSP to provide both complete accountability for message transactions and supportive documentation (reports, displays, etc.) detailing the system status and performance.

### 3.2.4.1 General Requirements

It is a requirement, by virtue of accepted standard TCC procedures and DoD Manual C5030-58M requirements, for a system of the CSP type to maintain complete accountability and an audit trail for all message traffic processed by the system. Such information consists of, but is not limited to, the quantity of messages, the time of receipt, from where the message was received, the size of the message (in lineblocks), security characteristics, the dissemination mode, and the time of transmission. This information provides a complete picture of the disposition of each message.

### 3.2.4.2 Hourly/Daily Statistics

The CSP keeps statistics on two types of traffic: the currently active traffic load and the message traffic history. A report for this is generated every hour, on the hour, and at the close of the RADAY. When RADAY is over, all the statistics are reset to zero. This report is called the Station Status Report.

The CSP also produces three other reports, generated at close of RADAY or by system operator commands:

- System History
- Transmission Line Logging
- History Log Report

### 3.2.4.3 Station Status

A report of the station status is generated every hour by the system. It contains the current system queue load:

- The number of lineblocks by device, precedence, and total for that device
- The atotal number of messages on the queue for the system
- The total number of lineblocks on the queue for the system
- The oldest active MLN
- The percentage of free queue nodes
- The percentage of free disk space

The queue statistics report is also generated at the close of the RADAY and can be obtained, at any time, by the operator.

### 3.2.4.4 Communications History

A sytem history report is the key element in the CSP system performance analysis.

The statistical communications history report is generated by the system at the close of RADAY; it can be obtained by the system operator at any time. The report contains the following information:

- The number of messages processed by a communication's device, by precedence, and the total for that device
- The number of lineblocks processed by a communication's device, by precedence, and the total for that device
- The total number of messages processed by the system
- The total number of lineblocks processed by the system

A report is generated for the receiving and transmitting devices. All statistical counts are reinitialized at RADAY change.

### 3.2.4.5 PLA Historical Usage

Information on the usage of Plain Language Addresses (PLAs) consists of the number of times each PLA was used, as well as a list and count of those PLAs encountered in a message, but not found in the PLA/RI conversion tables. The latter report is generated daily at RADAY change, while the PLA count report is generated weekly. Either report is obtainable upon request by the operator.

### 3.2.4.6 Dynamic System Status Display

The status of the CSP system is monitored constantly via the CSP dynamic system status display. A VT100 (or equivalent) terminal is used to display the status of the active lines, the current active message number range, the utilization percentage of the message file, the overall system status, and the time of day. Each line currently "on"

is monitored on the display, thus dynamically indicating line activity. The current number of messages on each output queue and any altrouting information is displayed.

### 3.2.4.7 Audit Trail

The following features provide the necessary audit trail capability which enable operation's personnel to completely evaluate system performance and trace the processing flow of specific messages.

#### 3.2.4.7.1 History File Logging (LOGGEN)

The most comprehensive message processing information is available through data reduction of the history file (disk or tape) maintained by the system. Utilities exist which allow the operator to reduce a history file to a printed log form, detailing every step to which each message has been subjected.

Due to the time-sequential nature of the history file, this log presents a chronological picture of system performance. Every processing state change that a message undergoes results in a data record on the history file. This is reflected in the log.

This utility may be executed either online or on an offline system, but the nature of the reduction process makes it very time consuming. Adequate thought must be given to allocating system resources for long periods of time.

#### 3.2.4.7.2 Communication Line Message Logging (LML)

On a line-by-line basis, users may specify that communications (Tor R) lines be logged. As each message is successfully transmitted to or received from a circuit, a log entry is made for that circuit. The information routed consists of the Originating Station Routing Indicator (OSRI), the station serial number (SSN), the date-time group (Format Line 5), the first 16 characters of the FROM line, the input and output channel desingator/sequence numbers, the time of transmission or reception, and the CSP accounting number. All of these parameters (except the FROM line) may be used as recall parameters in the event retransmission is required.

Summary log information is available through operator commands. At the end of the processing day (RADAY), complete logs are printed and the log files are zeroed for the next day. This feature has proven very useful in tracing activities and has, for the most part, supplanted the need to resort to a full history file log to ascertain disposition of

a praticular message. The total number of messages logged for a line is included on the daily report and is also printed on the system console.

### 3.2.4.7.3 Message File Logging

Message log information may also be obtained directly from the CSP message file. This can be accomplished very quickly and the type of information available is similar to that from the history log, with the following exceptions: log inforamtion may be specified for a single message or a group of messages based on the time of receipt of the receive communication's channel; the report generated cannot give as complete a picture of chronological activities (exact time of receipt, time of transmission) because the disk image represents a cumulative status of the message; and the messages available for logging can only range as far back as the oldest retrievable message in the system. This feature is particularly useful to traffic analysis personnel when evaluating the status or disposition of a single message or a limited group of messages, but it is rather inefficient for evaluating system performance over a period of time.

Selection of messages to be logged follow the same procedures and parameters as those of message recall, except that this function may be performed only from the system console.

## 3.2.5 System Security and Access

As described in paragraph 3.1.3.3, many physical security procedures are required to operate an accredited CSP system. Maintenance of a security environment is the responsibility of the TCC personnel. CSP provides many software features designed to augment physical control procedures. These features are described in the following paragraphs.

### 3.2.5.1 Input/Output Security for Communication Lines

Security classmarking is provided for every communication line defining security levels for that line. This classmarking information is used later to provide input/output security checking. All messages processed by the CSP system are categorized based on classification, compartments, transmission control codes, caveats, codewords, and language media format. Once the communication lines and message traffic have been marked with the appropriate classification, each message is checked against the level of the given communication line. Failure of these checks

results in message rejection. The message is marked as having failed the security check and is sent ot the Supervisor Review Queue for action.

### 3.2.5.2 System Access

In addition to software restrictions on message classifications, the system must preclude access of persons without the proper clearances and/or need-to-know. This is accomplished via user validation and physical access limitations.

#### 3.2.5.2.1 User Validation

Unauthorized users are prohibited from accessing various portions of the system by sign-on and password protection. Signing-on to the user terminal determines which remote offices and users are allowed on the system, and the functions they can perform. The password allows verification of each remote office with the user privileges. Functions are allowed or prohibited based upon these priviuleges. Controlled functions include: access to the supervisor review queue, the abiltiy to edit or delete a message, and the authorization to release messages originated by another input line.

### 3.2.6 System Tables

The CSP system contains elements identifying it as a unique entity to AUTODIN and defining its charactertics, as well as the local parameters, which allow it to differentiate among its backside users. These elements and parameters are organized in the following operational tables: routing indicators, routing segregation criteria, Plain Language Addresses, office symbols, user identification codes, and security data.

Each table is updated by running an offline utility program which accepts input from a disk file, card deck or terminal. An interim table is created and printed for inspection. The permanent table may then be replaced with the interim table, implementing the changes made. Tables should only be replaced with the approval of the Automated Message Processing System Security Officer (AMPSSI) or his designee.

Maintenance of each of the CSP system taables is discussed in detail in the following paragraphs.

### 3.2.6.1 Routing Indicators and Routing Segregation

Routing indicator tables are set up at system-generation time to reflect all local, CARP, and collective RIs for which the site is responsible. Messages addressed with RIs not found in these tables are transmitted to AUTODIN for delivery.

The system manager can change, add, or delete RIs for either the DSSCS or GENSER community. Note only ine (1) RI for each community should be specified for the delete-all-but action. These tables, however, must match those of the connected ASC. Changes to the RI tables are made via card or disk file input.

Since messages may be addressed to more than one destination, multiple RIs may appear on a message. To prevent the CSP and ASCs from redundant transmission of these messages, a table is set up at system generation time specifying which RIs will be deleted from and/or appended to Format Line 2 of the messages placed on the output queues. If the routing line segregatin criteria changes, or an output queue is added or deleted, the system manager changes the table using either card or disk input.

### 3.2.6.2 PLA

All Plain Language Addressing (PLA) tables are created and maintained through utilization of the Record Management Services (RMS-11) of IAS. The PLA data base is composed of indexed sequential files, which correlate a PLA with its routing indicator and an AIG/DAG with its set of routing indicators.

The system manager can add or delete PLA entries from the data base via card or disk file input.

### 3.2.6.3 Dissemination

Message dissemination is controlled by the communication's operator at the user terminal. This is done by a combination of techniques, including selection from a menu appearing on the user terminal and selection of a group of office symbols via the regular or variable function keypads. Automatic dissemination of messages is also supported, in certain cases. The following paragraphs describe the operational table maintenance required to support these functions.

### 3.2.6.3.1 Office Distribution Menus

Distribution office symbols are set up at system generation time ot reflect the offices and organizations served by each TCC receiving the most traffic. They are then displayed on the command screen and selected by light pen (OJ-389) or highlighting (Delta Data). Also, office symbols can be entered on the command line via keyboard entries.

If an organization is added, deleted, renamed, or the method of servicing is changed, these tables are modified by the system manager, using either card or disk file input. Additionally, if the office is on the CRITIC distribution list, the quantity value may be appended to the data field.

### 3.2.6.3.2 Automatic Routing

The Automatic Routing Data Base consists of a set of tables describing key messge elements and actions to be taken when the elements are found in a message.

Data base tables are maintained in individual source files in ASCII format. The system manager is responsible for keeping the tables updated as routing requirements change. When it is newcessary to update the online data base, a utility program is run to convert the source data base tables to an internal format and create directories to each of the tables. The source tables will be read and validated, ensuring that the format of each entry is correct and that the entries are in alpahabetical order. The new data base may then be loaded into the system either via a system start (cold/warm) or through the use of a utility program. Loading of the data base entails only the reloading of the directory areas since the actual tables are disk resident.

The following tables are used:

- Precedence Table
- Operating Signal Table
- Routing Indicator Table
- Transmission Control Code Table
- Addressee Table
- Delivery Distribution Indicator Table
- Format Line 12 Classification Table

- Format Line 12 Phrase Table
- GENSER or DSSCS Table

#### 3.2.6.4 User Identification

A table containing remote office, user ID codes, and user passwords is created at system generation time to identify the operators with access to the supervisor and the message distribution positions and operators with access to the message distribution position only. The user ID codes consist of operator initials and a shift identification or some other means of identifying a remote office and individual user; the remote office and user identification is appended to all messages processed by that user. Symbols for personnel with supervisor privileges are separated from other personnel symbols.

As user personnel are reassigned, arrive for duty, or are given additional access privileges, the system manager updates the remote office user symbol and password.

#### 3.2.6.5 Security

Two sets of security tables are defined within the CSP. The first, the security common area, defines all classifications, compartments, codewords, caveats, handling instructions and transmission control codes (TCCs) legal for messages processed by the CSP. The second security table specifies the allowed security parameters for messages processed by each (R or T) specific circuit/device/channel/line.

##### 3.2.6.5.1 Security Common

The CSP software is distributed in unclassified form and contains dummy data in all the security tables. At a system generation time, the system manager initializes the security tables to reflect the actual site level classification. This is done by placing the appropriate information in the classification, compartmentation, codeword, caveat, language media format, and TCC/SPECAT tables within the security common area.

##### 3.2.6.5.2 Circuit Classmarking

In order to ensure that a message transmitted to or received from a channel does not exceed the security parameters allowed for that particular line, a table is set up defining the maximum allowable security parameter for each line. These tables are set by the system manager at system

generation time to reflect, for each circuit, all classifications, caveats/codewords, TCCs, and LMFs allowable on messages transmitted to or received from the device/line.

If a new terminal is added or the security attributes of an existing channel are changed, the system manager updates the appropriate security tables via card or disk file input using the card reader, disk, or a terminal. When the input is from cards or disk, the security updates task assumes that an initialization of security tables is being performed and prohibits all elements for the specified device. Due to this prohibitive step, input data only specifies those elements which are to be allowed. Consequently, making minor updates is possible only through terminal input.

## SECTION 4. CONFIGURATION REQUIREMENTS

This section addresses the configurability of CSP and details the level of user configuration for a specific installation.

### 4.1 System Architecture

Prior to discussing specific parameters, a brief overview of the system architecture is in order. Figure 4-1 diagrams the major CSP modules, their inter-relationships, and the overall flow of message processing, generally left to right. Every item, except the Plain Language Expansion Module, the Automatic Dissemination module, and the Service Message Processor, are referred to as the "core" system. These components and their functions are fundamental to every CSP, regardless of application, and are not subject to configuration, except capability or table specifications. The other three items are either system options or directly involved in the configuration process. The single lines between modules (specifically System Management/Control functions) reflect the major operational control paths. The double lines denote message processing control transfer and are numbered sequentially, indicating normal process sequences. Paths 5a, 5b, 5c and 9 are contingency paths taken under varying processing conditions.

### 4.2 Configuration Parameters

The CSP was designed and developed to permit dynamic system configuration. The system manager has the necessary tools to perform system configuration in a timely manner, with no loss of message traffic. This capability includes, but is not limited to, initialization of all CSP system data structures and hardcopy output of the current system configuration. The system data areas included in dynamic configuration are communications lines, system output queues, operational terminals, system capacities, and optional routing characteristics.

#### 4.2.1 Communication Lines

The communications lines are the basis for the CSP configuration, the CSP was designed as a front-end or back-side processor of message traffic flow on these lines. The CSP maintains the necessary information to assure continued operation of all communication lines connected to the system.

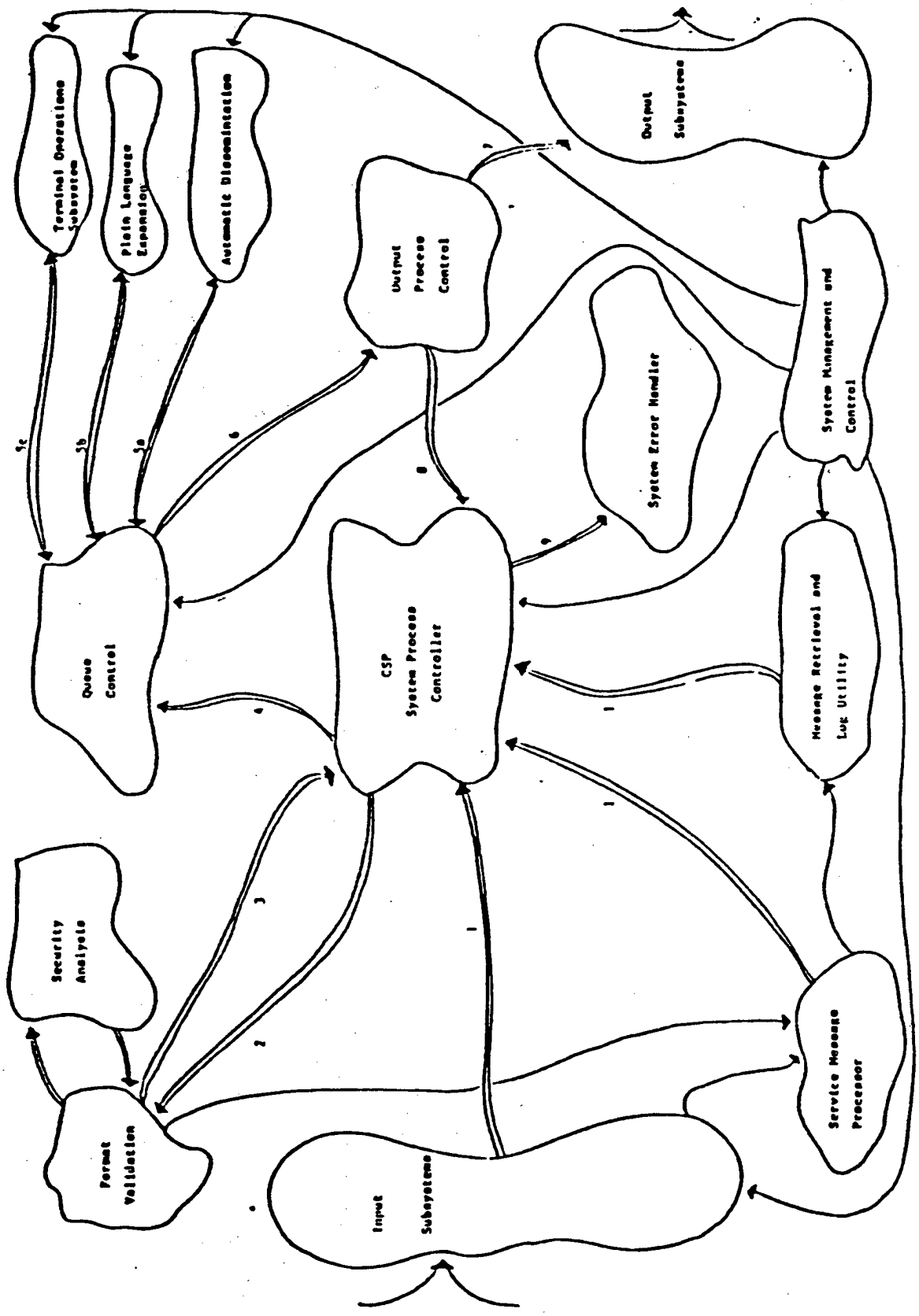


Figure 4-1 CSP Functional Baseline

Establishment and control of the communication line are handled by the CSP gateways. Each line is defined in CSPCOM as a gateway channel entry. Each communication line is assigned a name, a hardware device identification, a channel designator (if required), an output queue identification, and a system saturation shutoff value (input lines). As a minimum, the system can identify the line type and any characteristics of the line which necessitate exceptional processing, such as the channel sequence number of device specification modification.

The number of lines varies for any given site. All of the communication device/lines can be logically turned on or off by the system operator.

### 4.2.2 System Output Queue

The system output queue provides a waiting list for message traffic awaiting operator review, editing and dissemination, and CSP message transmission and hardcopy output.

The CSP maintains a queue for each output line defined in the system. Messages are placed on the appropriate queues, according to their assigned destinations, by the System Queue Manager. Messages leave the queues on the basis of first in first out (FIFO) by precedence.

The system queues are defined or configured with their associated output lines in the Gateway Channel Status Area. Each output queue is given a name, characteristics, a servicing task identification, and an alternate queue identification for altrouting purposes. For any given site, the number of queues varies.

### 4.2.3 User Terminals

Currently, the terminals supported by the CSP system and used by SSO communications personnel are one or more Sperry Univac OJ-389 and/or Delta Data 8260T terminals connected via a BR-1569/1731 communications multiplexer.

The basic function of the user terminal is to provide the SSO personnel control over the message traffic flow. Various combinations of terminal inputs allow the user to perform message dissemination and distribution, message servicing, and generation and editing of narrative message traffic. If required, the CSP can be configured without an user terminal. In this form, all traffic will be either derivatively routed or manually disseminated via hardcopy (after printing).

Definitions, statistics, and control of the operational terminals are contained in a system common area.

The CSP maintains all information required to ensure the continued operation of all user terminals. For audit trail purposes, this information includes current user identification. The system configuration parameters for operations terminals consist of the maximum number of user terminals. This number is used to allocate a sufficient areas of memory to contain status and accounting areas for each terminal.

### 4.2.4 System Capabilities

The CSP provides a system area containing definitions of system capabilities. System capacities are broadly defined to include message file size and device identifications, terminal paging file device identification, the maximum number of messages active in any output queue, the number of terminals on the system and the number of communication lines.

### 4.2.5 Optional Routing Characteristics

The CSP provides the capability for optional routing of certain types of messages and messages requiring hardcopy output for accounting purposes. Messages which require optional routing include those:

- In DOI-103 Modified format (DOI 103M)
- Generated at a terminal
- Of Category I
- Deleted by the Service Clerk
- Re-released by the Message Distribution Clerk
- Containing undefined disseminees
- Containing no disseminee
- Routed to the default routing by online message recall

## 4.3 System Installation Options

The various operational parameters vary from one location to another. An example of this condition is the minimum length of the local routing indicator definitions. Some locations may key off of four characters, while others may use five. The CSP provides the capability to modify these parameters, in a manner requiring the least amount of programmer involvement. Two separate, but similar, functions at the same location may require different parameters.

Parameters defined by site requirements are:

- Maximum number of messages written to an intercept device
- Maximum number of message read from an intercept device
- Number of lines per page for distribution and service printers
- Width of print line for service printer
- Maximum number of messages recalled by online message recall
- Minimum length for local routing indicator definition
- Ability to disable security sentinel and OSRI validation
- Block size for magnetic tape interfaces
- History device retention period
- Ability to secure a hardcopy of all messages deleted from the system
- Percentage of message file in which online recall is prohibited
- Length of time between time hacks
- Ability to class stamp service printer traffic
- Ability to print multiple copies of a message
- The time of day to print the PLA statistics

- Ability to allow release of a message previously disseminated or containing no dissemination
- Ability to obtain a courtesy copy of various types of messages
- Ability to modify the scan parameters in the automatic routing module
- Ability to define altroutable queues and queues that an altrouted queue can be altrouted to.

# SECTION 5. SYSTEM ENVIRONMENT

This section describes the hardware and software environment in which the CSP operates.

## 5.1 Hardware

The minimum hardware configuration which supports the CSP is shown in Figure 5-1. Each element of this configuration is discussed below.

### 5.1.1 CPU, Memory and System Console

The CSP is capable of running on the central processing units (CPUs) of the Digital Equipment Corporation (DEC) PDP-11 family, within the 11/34 to 11/70 range. In its minimum configuration without PLA or FARM, the baseline CSP runs in 256KW of system memory (including 60K words for the executive and standard device handlers). Memeory usage in the 256KW word range occurs during peak processing.

The system console is the only device permitted to interact with a control the system. It must be a hardcopy terminal, such as a DECwirter (or equivalent).

### 5.1.2 Mass Storage

The CSP requires both disk and/or tape devices (tape devices are not required if dual-disk recording redundancy is used) for mass storage. The utilization of these devices is described in the following paragraphs.

#### 5.1.2.1 Disk

Online disk storage is required for both operational CSP software ad the system message file. Approximately 10 megabytes are required for the CSP software. The number of megabytes required for the message file is dependent upon the volume of traffic and the number of days that back traffic will be maintained. An additional 40 megabytes of disk storage is needed to support the CSP software in maintenance form (sources, objects, listings, etc.).

Although it is possible to run CSP with only one drive, separation of the software and message file greatly improves disk access time. If possible, two drives should be dedicated to CSP use. One 10 megabyte disk is adequate for the CSP operational software. The size of the second disk is contingent upon the size of the message file; it may range

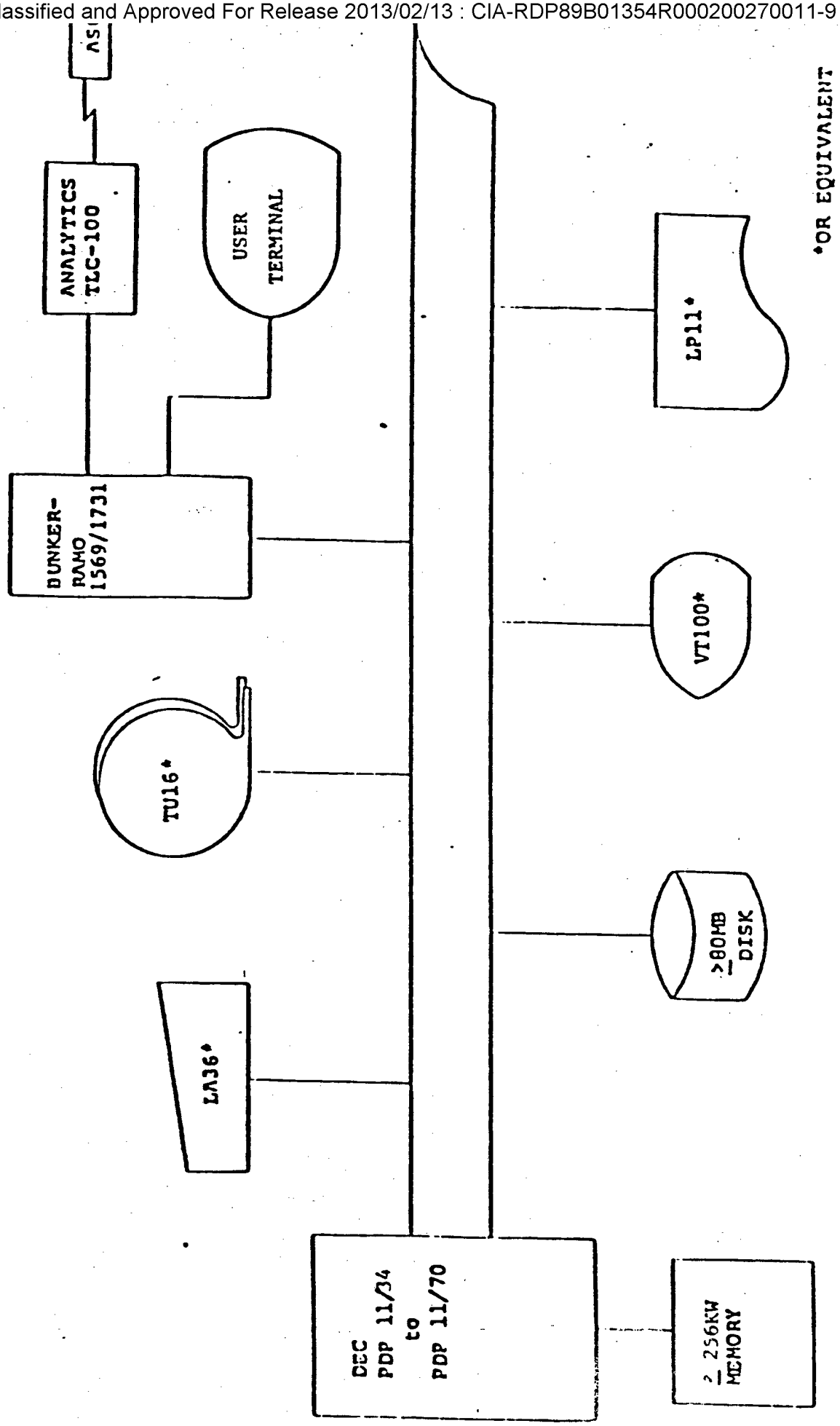


Figure 5-1 Minimum CSP Hardware Configuration

from 30 to 3000 megabytes. In order to support system maintenance, one of the drives must accommodate a minimum of 80 megabytes.

#### 5.1.2.2 Magnetic Tape

If a site is not using dual-disk redundancy recording, a minimum of one magnetic tape is required for history file recording of the message traffic. Additional tape drives can be configured, one for the online history tape and the remainder for either history pre-mount and/or intercept tapes.

If sites are using a dual-disk redundant recording configuration, magnetic tape drives are not required unless the site desires offline tape capabilities.

Additional tape drives may be used to decrease the workload involved in mounting/dismounting tapes when in-use drives are needed for intercept tape, or to support magnetic tape circuits (if so configured).

Inputs to and output from the CSP maybe received/transmitted in 80 character data pattern (card image) format on 9-track tape. Only standard DSSCS/GENSER narrative format or OCR format (if a PLA capability is present) messaes may be meaningfully transferred in this manner.

### 5.1.3 Communication Interfaces

The CSP supports a variety of devices for communicating with AUTODIN, NSA, ZICON, Mode II, the user terminal, backside/front-end processors, and site unique devices/lines. The hardware devices available for communication link support are described below.

#### 5.1.3.1 Communication Interfaces

The BR-1569 (and its successor, trhe BR-1731) 32-channel communications multiplexer is capable of providing communicatoin links for the majority of CSP interfaces. The configuration of the BR-1569/1731 is selected during procurement and is based upon existinag and projected communicaiton requirements.

#### 5.1.3.2 DMC11

The DMC11 Network Link provides a synchronous computer-to-computer link over coaxial/triaxial cable or via synchronous modems. This capability is used to link CSP systems together or to access backside computer systems.

#### 5.1.3.3 Other Interfaces

Several other communication devices are supported by the CSP. The DUP11 is a single line synchronous device; the DV11 is a synchronous/asynchronous eight or sixteen channel multiplexer. Any one of these devices can be included in a CSP hardware configuration.

### 5.1.4 AUTODIN Interface Devices

In addition to the communications devices described above, the CSP utilizes an AUTODIN interface device to communicate with the AUTODIN Switching Center (ASC). Devices such as the Analytics TLC-100 or the INTEQ are used for this purpose.

### 5.1.5 Line Printers

Line printer(s) are used to print all hardcopy forms of message traffic and statistical reports produced by the CSP. Two logical printer devices are defined by the CSP; one is used for the distribution form of message traffic and the other for the statistics and service forms of message traffic. DEC LP11s or equivalents may be used for this purpose.

### 5.1.6 Other Peripherals

Other peripherals used with the CSP are described below.

#### 5.1.6.1 Card Reader

The CSP supports message input via a card reader. The DEC CR11 or equivalent may be used. The card reader is optional.

#### 5.1.6.2 Paper Tape Reader/Punch

The CSP can process messages via ASCII paper tape, using the DEC PC11 or an equivalent reader/punch. The CSP also provides Mode II BAUDOT paper tape support. Inclusion of a paper tape reader/punch is optional.

#### 5.1.6.3 Optical Character Reader

The CSP supports the use of a "dumb" OCR for message input in DD 173 format. Any "dunb" OCR may be used. The OCR is optional.

#### 5.1.6.4 User Terminal

User terminals (OJ-389 or Delta Data 8260T) will be used by the TCC personnel for : message dissemination and distribution; message servicing; and the generation and editing of traffic. One terminal is sufficient for minimal control, with personnel switching between message distribution and service functions. Additional terminals (up to 6) may be added to decrease contention and increase throughput. The CSP may be configured without user terminaals if required, although this is not a typical configuration. With this latter form, all traffic will either be derivatively routed or manually disseminated (after printing).

#### 5.1.6.5 VT100/Equivalent

The VT100 (or other CRTs, such as VT52) is used as a slave terminal for the system status display program. Continuously updated status of the system and its components is displayed. A VT100 (or the equivalent) is a requried peripheral.

#### 5.1.6.6 Magnetic Tape

Inputs to and outputs from the CSP are received/transmitted in 80 character data pattern (card image) formats on 9-track tape. Only standard DSSCS/GENSER narrative format or OCR format (if a PLA capability is present) messages may be meaningfully transferred in this manner.

### 5.2 Software

The following paragraphs detail the characteristics, organization and restrictions pertaining to CSP software development, support, maintenance, and operation.

#### 5.2.1 Operating System

The software comprising CSP can be viewed as an applications package and, as such, must rely upon a resident operating system for hardware and software services necessary to perform its functions. Most operating systems can be divided into two major functions:

- Executive services, covering program scheduling and execution, as well as program services ranging from inter-task communication to task input/output.

- Peripheral device interfaces allowing application program access to various hardware components (disk, tape, terminals, etc.) without requiring those programs to directly interface the devices. Both of these aspects are covered more fully in the following paragraphs.

#### 5.2.1.1 Executive

The executive for which CSP was designed and coded is the Digital Equipment Corporation Interactive Application System (IAS), Version 3.2. IAS is a multi-tasking, real-time operating system providing a full range of services necessary or desirable for real-time applications.

IAS can be configured in one of three ways. A minimum size, single user system; a larger, multi-user system capable of serving many users simultaneously; and a timesharing version, supporting up to 64 users in a timesharing mode while still providing real-time services to tasks requiring them. CSP uses the multi-user version of IAS, although it is viewed as a single integreated package of application programs.

#### 5.2.1.2 Device Drivers

Standard DEC and Bunker Ramo device drivers are utilized to interface with CSP peripherals as follows:

| Component | DEC Driver(s) |
|---|---|
| Disk | DB...., DP...., etc. |
| Tape | MM...., MP.... |
| Paper Tape Reader | PR.... |
| Paper Tape Punch | PP.... |
| Card Reader | CR.... |
| Printer | LP.... |

| Component | Bunker Ramo Driver(s) |
|---|---|
| BR-1569/1731 | BM.... |
| User Terminal | UT.... |

#### 5.2.1.3 Constraints

CSP utilizes the standard IAS system and device drivers. No modifications are made to either the operating system or the device drivers.

The IAS operating system is installed in accordance with the installation and system generation procedures outlined in the IAS System Generation and Startup Guide published by DEC. The actual configuration of the IAS system is site dependent and will vary according to specific needs of the user.

### 5.2.2 Development Base

The basis for development of all software for the CSP system is version 3.2 of the IAS operating system developed by Digital Equipment Corporation (DEC). IAS is a real-time operating system which allows concurrent, hardware protected execution of multiple online tasks. Complete utilities include a MACRO assembler, task builder, editor, debugger, and the file utility programs.

#### 5.2.2.1 Language

All CSP software is written in MACRO-11 assembly language, except FARM which is written in FORTRAN. MACRO-11 is described in the IAS/RSX-11 MACRO-11 Reference Manual produced by DEC.

#### 5.2.2.2 Constraints

DEC IAS and MACRO-11 conventions are followed throughout CSP software development.

### 5.2.3 System Organization

In normal installations, the CSP consists of two separate systems. The first is a complete CSP system package, including maintenance tasks and utilities. The second is the operational configuration. The following paragraphs described the circumstances under which each of these systems is used.

#### 5.2.3.1 Development Mode

The CSP package consists of the complete IAS package, CSP object modules and command files for building CSP. This package is used for the installation of the CSP as well as test and checkout of the system at any time. Modifications or updates to the system (either IAS or CSP) must be made to this system package.

#### 5.2.3.2 Operational Mode

The operational system is created from the maintenance and development system and is used operationally. It consists of only those files needed to run the system. This is to say that only software (mostly task images) required for CSP operation is included. As a system, it is only capable of the CSP function and is unable to support program development, debugging, modifications, etc. THE SECURITY ACCREDITATION OF THE CSP IS BASED ON USE OF THE OPERATIONAL PACK ONLY.

### 5.2.4 Software Transfer

Software distribution is accomplished via magnetic tape or disk when a site is configured without tape drives. CSP distribution tapes contain CSP baseline software, optional software modules as required for individual sites and indirect command files. The CSP software from the distribution tape must be transferred to and merged with the CSP maintenance system \9CSPMAD). This is accomplished by executing the indirect command files contained on the distribution tape. The command files utilize the IAS FLX utility to accomplish the physical transfer between tape and disk. The command files ensure that all software from the distribution tape is properly merged with the maintenance system.

When a site has a configuration without magnetic tape drives, the software distribution file is sent to them on disk.

## SECTION 6. MANAGEMENT REQUIREMENTS/SYSTEM DEVELOPMENT PLAN

Accreditation, enhancement, maintenance and distribution of the CSP requires the application of systematic software management techniques. This section describes techniques which are utilized in CSP management.

### 6.1 Accreditation Including the Test Plan Update

Prior to the operational acceptance and security accreditation of the CSP, several criteria must be satisfied. Accreditation includes not only hardware and software, but also site preparedness, physical TEMPEST and personnel security, and operator proficiency. To evaluate these areas, it is necessary to perform a series of tests from a standard published CSP Accreditation/Certification Test Plan and Procedures document. The Plan includes sufficient tests, with expected responses for each, to evaluate the entire CSP system (reference paragraph 1.3.1.7).

The accreditation and operational acceptance of the CSP is actually two separate processes; the same Test Plan is used to satisfy both. Security accreditation is granted by DIA upon successful completion of all test groups, focusing primarily on the security aspects of the system. Operational acceptance is granted by DCA upon successful completion of the Category III AUTODIN interface test, concentrating on the integrity of the data introduced into the AUTODIN system.

### 6.2 Configuration Management

The Configuration Management (CM) Program plays a critical role in governing the evolution of the CSP throughout its life cycle. In order to accomplish this task, the CM Program:

- Identifies and documents CSP baseline configurations which emerge as part of the system development process.
- Ensures that interfaces between the CSP and other computerized systems are properly developed and maintained.
- Establishes and maintains mechanisms for identifying baseline and site-unique documentation, software modules and hardware configuration.

- Provides mechanisms for proposing, tracking and verifying all levels of changes to CSP elements.

- Ensures orderly development, integration, testing/validation, and dissemination of centrally or site-identified additions/modifications to the software and/or its documentation.

- Monitors idendification, resolution and testing of software/documentation errors or deficiencies and the orderly dissemination of corrections to the user sites.

- Conducts reviews and audits as required to ensure conformance to specifications.

All new software modules are reviewed by the Informatics Project Manager upon completion, and when accepted by the AFIS/IND Project Manager, made a part of the CSP baseline. Once part of the baseline, these modules are available for installation at additional sites where a common requirement exists. All specifications, software, firmware, hardware, and documentation which have been accepted as part of the general CSP baseline, or any site tailored baseline under configuration control, are not altered without first being processed and approved using standard configuration management procedures.

All changes that occur once the configuration identification has been established are classified into two categories: Class I or Class II changes. A change is Class I if it affects:

- A techenical requirement or specification in the functional baseline

- The project schedule or cost

- The software design, performance, or external interfaces

All changes which are not Class I, including editorial and program error correction are Class II changes. The minimal approval authority for Class I changes is the AFIS/IND Project Manager and, when deemed necessary, the Configuration Management Board (CMB). Class II changes may be implemented without prior approval of the CMB, but are controlled and reported in accordance with the remainder of this subsection. In any case, the Informatics Project Manager is the minimal approbal authority for all Class II changes.

Standard CUBIC Probelm Reports (CPR) are utilized as necessary. Part I of the CPR is filled out by the originator; part II, by the AFIS/IND project officer or his representative; parts III by the originating organization to indicate completion. These procedures enable users to submit requirements for development of required software, facilitate consideration of such requirements on a common-user basis, and establish a process for evaluation and integration of community-developed softwre satisfying common user requirements.

The tools used to assist the configuration management process can enhance or destroy the effectiveness of the CM system. In order to be useful, CM information must be systematically and accurately recorded. Retrieval must be both fast and flexible. Informatics has developed, as an in-house tool, an automated Configuration Management System (CMS) which meets these criteria. The CMS is used to maintain complete CSP baseline and site inventory information and to perform problem logging.

### 6.3 Software Quality Assurance (SQA)

Software Quality Assurance, or quality control, monitors the development and performance of the system throughout its lifecycle. The SQA Program is concerned with every aspect of the analysis, design, development, testing, implementation, documentation, training and operational support of the CSP system.

The goals of the Software Quality Assurance Program are aligned with the goals of the Configuration Management Program, as both programs are used to monitor and control the software and documentation produced in the CSP development effort. The Software Quality Assurance Program is primarily concerned with the quality of the product, whereas the Configuration Management Program focuses upon the configuration status ofthe baseline and site CSPs.

The CSP Software Quality Assurance Program establishes a structure which is imposed on CSP development, providing an efficient path for the ensuring the quality and timeliness of the overall product.

Several tools are used to help guarantee the integrity of the CSP software. These tools fall into three categories: development aids, which allow simulation of real environments in an artificial test setting; and security accreditation, which assures that the code integrity is maintained at a level in conformance with government specifications. All

aspects of the SQA Program assure that the system product will be developed, maintained, and updated in accordance with the highest standards.

### 6.4 Maintenance

Informatics has an established problem reporting structure and a software maintenance team capable of responding quickly to all reported problems. The cycle is initiated with recognition of a CSP malfunction, apparently attributable to software, by operations or user personnel at a CSP installation. AFIS/IND will be informed of a software malfunction by the issuance of a CUBIC Problem Report from the CSP site where the problem was encountered. Upon validation of the problem report by AFIS/IND, Informatics will be notified and will begin diagnosing the problem based upon information in the report, supplemented as required by telephone conversations with on-site operations and user personnel.

If the problem analysis conducted by Informatics indicates that a software error exists, required corrective actions will be determined and the resulting maintenance task will be sized and scheduled. AFIS/IND will be provided information concerning the diagnosis results, scheduled corrections, and an estimated completion date. This notification will occur within five (5) working days of receipt of the problem report.

Once a software fix has been designed, thoroughly tested and evaluated, it will be incorporated into the baseline and distribution made to AFIS/IND and to the appropriate installations. All CSP modifications involved in software maintenance activities will be developed, implemented, tested and documented in accordance with the CSP Quality Assurance Program and CSP Configuration Management Plan. In addition, the status of all CUBIC Proglem Reports will be monitored from start to finish by the Informatics-developed automated Configuration Management System.

If the urgency of the problem does not permit the above procedures to be followed, interim solution or circumventing procedures may be instituted as a result of advice from on-site or central support personnel after coordination with the Project Manager and AFIS/IND. Once operational capabilities are restored, a CUBIC Problem Report will be submitted. Formal problem resolution steps will then be taken to ensure a complete, tested, integrated and documented solution. After this solution is disseminated, the interim solution will be removed and the official correction applied.

## 6.5 Updates

All new software modules are reviewed by the Informatics Project Manager upon completion, and when accepted by AFIS/IND, made a part of the CSP baseline. Once part of the baseline, these modules are available for installation at additional sites where a common requirement exists. All specifications, software, firmware, hardware, and documentation which have been accepted as part of the general CSP baseline, or any site tailored baseline under configuration control, are not altered without first being processed and approved using standard configuration management procedures.

As major enhancements to the CSP are developed and successfully implemented in the CSP baseline, they are distributed to AFIS/IND for distribution to the appropriate CSP installations. Depending upon the complexity of the enhancement and the expertise of on-site personnel, the distribution procedure varies. For minor enhancements, update tapes are sent to AFIS/IND for distribution along with supporting documentation for installation. For extensive enhancements and sites with no resident software support personnel, the upgrade is installed by contractor personnel.

Software releases are scheduled periodically and contain all new software and patches accumulated to a cut off date which will generally be no more than one month prior tot he release date. In any case, the cutoff date will be specified in the accompanying release notes.

The software is accompanied by appropriate documentation, release notes, and status reports. The release notes include descriptions of any new software (including name and module revision code), a description of any problems, installation and test instructions, and any new operational considerations of which the user should be aware. Accompanying status report detail the status of other change requests and developmental activities.