GBPPR 'Zine Image: Constraint of the American Hacker Image: Constraint of the American Hacker



Don't get it ->

"Democracy, immigration, multiculturalism. Pick any two."

--- James C. Bennett, at the end of a post on Australia's Sydney beach riots.

Table of Contents

- ♦ Page 2 / Introduction to Software Descriptions / #1A ESS
 - ◆ It's a little more complicated than a Speak & Spell.
- ◆ Page 51 / Portable Video Camera Viewer
 - Device to visually test a video camera's output signal.
- Page 57 / Micky "Cheesebox" Callahan
 - Excerpt from the book Cheesebox Callahan.
- Page 64 / Using the Alternative Enhanced Redirect Service Data Validation Tool
 - Update your business line routing in case of an emergency.
- ◆ Page 70 / How to Break Into Medium-Security Installations
 - Old file from the local BBS scene.
- ◆ Page 78 / Nortel DMS-100 Input/Output Device Maintenance Overview
 - Input/output device maintenance overview under a DMS-100.
- ◆ Page 91 / Motorola Bag Phone Handset Control
 - Control a Motorola cellular phone's handset with a simple PIC circuit.
- ♦ Page 106 / Bonus
 - Wanted.
- + Page 107 / The End
 - Editorial and rants.

AT&T PRACTICE SPCS

-

Ţ

ų i

AT&T 231-045-000 Issue 3, June 1984

INTRODUCTION TO SOFTWARE DESCRIPTIONS 2-WIRE 1 AND 1A ``ESS^{*}'' SWITCHES

	CONTENTS	PAGE	CONTENTS PAG	GE
1.	GENERAL	2		8
		2		8
	PURPOSE AND CONTENTS OF 1/1A ESS		1A PROCESSOR ASSEMBLY LANGUAGE	10
		. 3	MACROS	10
	A. Section Numbering Plan		ESS SWITCH PROGRAMMING LANGUAGE	
	B. Program Coverage	3	(EPL)	11
	C. Support Documentation	3	DIAGNOSTIC LANGUAGE (DL-1)	11
	SCOPE OF SECTION	3	DATAPOOL	11
	ATTACHED PROCESSOR SYSTEM	3	PROGRAM DEVELOPMENT PROCESS	12
	CARRIER INTERCONNECT	3		12
2 .	INTRODUCTION TO PROGRAM CONTROL	4		13
	GENERAL	4	4. PROGRAM STRUCTURE OVERVIEW	14
	MEMORY	4	GENERAL	14
		5	INTERRUPT SYSTEM	14
	BUS SYSTEMS	5	INPUT/OUTPUT MAIN PROGRAM	14
		5	A. Introduction	14
	A. General	5	B. Characteristics	15
	B. Instruction Execution	5	C. Organization	16
	C. Data and Address Generation	6	5. BASE-LEVEL PROGRAMS	16
	D. Processing	8	GENERAL	16
3.	PROGRAMMING LANGUAGES AND DOCU- MENTATION	8		17
* т	ademark of AT&T Technologies		6. ORGANIZATION OF 1/1A ESS SWITCHES SOFTWARE SECTIONS	17

AT&T TECHNOLOGIES, INC. - PROPRIETARY

Printed in U.S.A.

Page 1

AT&T 231-045-000

	CONTENTS		PAGE	
	GENERAL			17
	FUNCTIONAL ORGANIZATION OF 1/1A SWITCHES SOFTWARE DESCRIPTIONS	. ES	is	17
	DESCRIPTION OF CONTENTS-1/1A SWITCHES SOFTWARE SECTIONS	E S	is	18
	SECTION-TO-PIDENT CROSS-REFER	:NC	ж	18
	PIDENT-TO-SECTION CROSS-REFER	:NC	:Е	18
7.	ABBREVIATIONS AND ACRONYMS .		•	18
Figur	es			
1.	Central Control With External Commu	nitie	es	
•		•	•	4
2.	Central Control Overview	·	•	0
3.	Decode, Control, and Address Formati	on		7
4.	Operation Circuitry			9
5.	Program Development Process	•		13
6.	Program Control Plan		•	15
7.	Input/Output Main Program	•		17
8.	Organization of 1/1A ESS Switches ware	Sof	it-	19
Table	25			
A .	Interrupt Levels	•	•	16
B.	Description of Contents—1/1A Switches Software Sections	E !	5S	23
С.	Section-to-Pident Cross-Reference .		•	33
D.	Pident-to-Section Cross-Reference .		•	50

1. GENERAL

INTRODUCTION

1.01 This section provides an introduction to the 1 and 1A ESS switches software and the Software Descriptions which describe the functions of the software programs. It provides information that is common to both the 1 and 1A ESS switches and information that is peculiar to the 1A ESS switch only. Any information that is peculiar to a 1A ESS switch is noted as such. Information that is peculiar to the 1ESS switch is not given.

- 1.02 This section is reissued for the following reasons:
 - (a) To include a brief description of these sections in Table B:
 - 231-045-440
 - 231-045-445
 - 231-045-455
 - 231-045-460
 - 231-045-490
 - (b) To delete from Table B sections 231-045-425 and 254-280-240
 - (c) To delete major portion of Part 5
 - (d) Figures 8, 9, and 10 removed
 - (e) Addition to old Fig. 11 now Fig. 8
 - (f) New pidents are added and others deleted from Table C
 - (g) Obsolete Table D completely revised

 (h) To add information concerning the attached processor system using the AT&T 3B20D
 Model 2 computer

(i) To add information concerning the Carrier Interconnect.

Change arrows are used to denote significant changes.

ISS 3, AT&T 231-045-000

1.03 Part 7 of this section provides a defined list of abbreviations and acronyms used in this section.

PURPOSE AND CONTENTS OF 1/1A ESS SWITCHES SOFT-WARE SECTIONS

A. Section Numbering Plan

1.04 Software sections related to the 1/1A ESS switches are designated by the following number plan:

NUMBER DESCRIPTION

- 254-280-XXX 1A processor programs/reference manuals common to 1A ESS switch and other systems (eg, 4ESS switch).
- 231-045-XXX Software Descriptions which provide information that is common to both 1 and 1A ESS switches. Information that is peculiar to the 1A ESS switch only is also included when necessary. Information that is peculiar to 1ESS switch only is not included.

231-310-XXX Software Descriptions applicable to 1A ESS switch only.

The last three digits in each series further designate the functional positions of the document within the overall 1/1A ESS switches software coverage. A complete listing of the documents relative to 1/1A ESS switches software is given in Part 6 of this section.

B. Program Coverage

1.05 Software Descriptions provide high-level descriptions of major software functions. Many of the documents encompass two or more separate programs when these programs together perform the major functions to be described. The purpose of each document is to provide:

(a) The purpose and structure of the program(s)

(b) Explanations of the primary functions at each appropriate level within the program structure (c) Identification of interfacing programs and interprogram relationships.

C. Support Documentation

1.06 In addition to the above, each description identifies the pertinent program entry/exit points to enable the reader to easily access the program listing for all further level of detail required.

1.07 Support documents (sections) are provided to serve as reference manuals for all source languages used to develop these programs, description of the program listings, various library listings, and other reference manuals.

SCOPE OF SECTION

- **1.08** As a high-level introduction to 1/1A ESS switches software, this section provides a brief description of:
 - (a) The 1A processor central control with emphasis on execution circuitry and registers which are directly referenced in program instructions.
 - (b) The source programming languages, including the assembly process and program listings.
 - (c) The overall system program structure of the 1/1A ESS switches. Cross-reference lists of all programs covered in this series with the sections in which the programs are described are also provided.

ATTACHED PROCESSOR SYSTEM

1.09 The attached processor system is used to replace the file store. The attached processor system consists of a 3B20D Model 2 computer using a 160 Megabyte disk system and an attached processor interface frame.

CARRIER INTERCONNECT

1.10 The Carrier Interconnect feature provides inter-LATA (local access and transport area) carriers and international carriers access to local exchanges via 1 and 1A switches. Basically, the Carrier Interconnect feature provides the data and program logic necessary to route calls to and receive calls from inter-LATA carriers. The LATA is a defined geographical area where equal access and of-

AT&T 231-045-000

fices and/or access tandems can provide an inter-LATA carrier/international carrier access to the local exchange. Calls between LATAs are handled by an inter-LATA carrier. This feature is not provided for HILO networks.

2. INTRODUCTION TO PROGRAM CONTROL

GENERAL

2.01 Program control of the 1A ESS switch is performed by the 1A processor which is made up of four communities of external units and a central control unit (Fig. 1). Private-access buses connect each community with the central control.

2.02 Two of the communities provide the primary memory for the central control. The program store memory contains some fixed control data and the bulk of the program instructions executed by the central control. The call store memory contains fixed control data and record type data which may be interrogated and updated during program execution. The call store memory contains more fixed control data (eg, translation data) than program store memory. High speed storage is provided on disk in the file store or attached processor system. Additional bulk storage is provided by tape transports in the auxiliary data system.

2.03 The auxiliary unit community is made up of units which are capable of communicating with program store and call store communities via central control bus access circuitry. The units control access to bulk memory and data links. The peripheral unit community consists of the switching equipment and associated access control circuitry. It includes the TTY units, the Master Control Center (MCC), the processor peripheral interface (PPI), and various types of network, scanner, and signal distribution units.

MEMORY

2.04 The program store and call store memory are available in 65K word stores and 256K word stores. The following is a brief description of the 65K word stores. (A similar description for 256K stores is a store of the store

word stores. (A similar description for 256K stores is provided in section 254-201-015.) The program stores and call stores are physically identical memory stores. The capacity of each store unit is 65,536 twenty-six bit words (24 bits of data and 2 bits for parity). Each store unit consists of two modules. The access circuitries for program store and call store are basically identical with the exception of the size of the reply bus. The program store reply bus which concurrently accesses both modules of a program store unit on a read order returns 54 bits of information (48 data bits, 4 parity check bits, an all-seems-well bit,



Fig. 1—Central Control With External Communities

and an all-seems-well failure bit). The call store reply bus which accesses one module of a call store unit on a read order returns 28 bits of information (24 data bits, 2 parity check bits, an all-seems-well bit, and an all-seems-well failure bit). The program stores are not duplicated, but are all backed up on disk in the file store or attached processor system. Besides the program store units required to store the generic program, two program store units are designated as spares. The call stores contain transient call-related data and semipermanent control data such as translations and data tables. The transient data is usually duplicated in another store. Translations and data tables are located in a protected area of the call store which requires a special instruction to overwrite. This data is not duplicated but is backed up on disk backup

AUXILIARY STORAGE

2.05 Bulk storage for the 1A processor is provided on magnetic disk and tape units accessed by the auxiliary unit bus system. This bus system has two terminations:

- (a) One at a disk backup or attached processor system.
- (b) The other at a data unit selector which, in turn, interfaces with the tape transports.
- **2.06** The file stores or attached processor system is used primarily for storage of:
 - (a) Nonduplicated program and call store contents
 - (b) Infrequently used programs
 - (c) Data which is paged into program and call stores when required for execution.

The information stored on tape serves as a final backup for the 1A ESS switch. All the information that is necessary to resume normal call processing, after a severe interrupt, is stored on tape. This information includes translation data, parameter data, library programs, program store contents, and essential data in call stores.

ISS 3, AT&T 231-045-000

BUS SYSTEMS

2.07 The four major bus systems of the 1A processor are shown in Fig. 1. Two-way communications between central control and all units are provided on two separate buses:

- (a) A write bus to send data from central control to a unit
- (b) A reply bus on which to receive data at central control.

In order to address any particular unit, all address buses include an enable code field designated as the K-code, which specifies the unit being addressed. The remaining bits on this bus then specify the location within the unit and the type of operation. For example, the call store address field includes:

- (a) A 5-bit K-code which specifies one of the call store codes $% \left({{{\mathbf{x}}_{i}} \right)^{2}} \right)$
- (b) A 16-bit address which specifies one of 32,768 words in this store module. Each bus group includes control buses not shown in Fig. 1 for transfer of maintenance, control, and status information.

CENTRAL CONTROL

A. General

2.08 Each 1A ESS switch office has two central control frames. These are duplicates of each other and operate in step, one in the active mode and the other in the standby mode. When a mismatch of the data being processed is detected, the one containing the error condition can be repaired while the other central control continues to process all calls. The primary function of the central control equipment is to read the program instructions from memory, to decode them, and to execute them.

B. Instruction Execution

2.09 An outline of the basic components of the central control involved in the execution of program instructions is shown in Fig. 2. Instructions are read from order memory (order and program instructions are used interchangeably) which is normally in the program store (although the central control is capable of reading orders from the call store). The

AT&T 231-045-000

central control continues to read instructions until a transfer in control is encountered, in which case reading continues with the destination address of the transfer. The instructions are either 1-word or 2word instructions.

2.10 The decode, control, and address formation circuitry decodes the binary information in the order word and controls the execution accordingly. Various fields of information (groups of bits) are sent to appropriate circuitry within the central control. A more detailed diagram of this circuitry is in Fig. 3.

C. Data and Address Generation

2.11 The execution of most 1A ESS switch orders requires the generation of a data word or a memory address. Several factors influence this address or data generation. In general, a data field in the order is added to the contents of an index register in the index addre circuitry. The results replace the contents of the data address register (DAR) (see Fig. 3). If this result is to be used as data, it is sent directly to the operation circuitry. If the result is used as an address, it is interpreted by the memory address decoder which determines the memory community to be addressed.



Fig. 2—Central Control Overview

ISS 3, AT&T 231-045-000





AT&T 231-045-000

D. Processing

General

2.12 Two internal central control buses, the masked bus and the unmasked bus, are the paths for information enroute to and from central control registers. The central control registers are fast-access flip-flop memory and may be accessed several times during the execution of a single program instruction. They consist of 24 bits which are numbered from the right, beginning with the least significant bit 0 to the most significant bit 23.

General Purpose Registers

2.13 The index registers, designated as the F, G, J, K, X, Y, and Z registers, are the general purpose registers which can be specified as the source or destination of an operation as well as a source for indexing in address information. The logic register serves as a special purpose register to receive all peripheral unit replies and to perform a specific function in certain logic operations.

Special Purpose Registers

- 2.14 Some of the special purpose registers and their functions are:
 - (a) Data Buffer Register B: A register whose contents always reflect the last data word read from or written into the data memory.

(b) Top-of-Stack Register T: A register which always contains the top or most recent entry in the Pushdown Stack, located in the call store, which is used for program transfers, ♦but may also be used for temporary data storage.

(c) P Register: Peripheral data register (36 bits) used for transmitting data and instructions to peripheral units on the peripheral unit write bus.

(d) E Register: A register which registers the name of the peripheral unit enabled to receive data.

(e) Control Flip-Flops (CF): Two flip-flops which are set at the completion of an arithmetic, log-

ical, or ϕ memory-read ϕ operation to show the result as positive or negative and homogeneous (all ones or all zeros) or nonhomogeneous.

Page 8

2.15 The logical or arithmetic functions in the execution of a program instruction are accomplished in the operation circuitry. These functions may include add, compare, logical product, logical union, exclusive-OR, rotate, shift, complement, rightmost-one detection, insertion, or some combination of these functions. These operations can have one or two 24-bit arguments (operands), which can come from a memory location or a data field of the program instruction and/or a central control register. Figure 4 gives a more detailed view of the operation circuitry and examples of instructions which utilize the circuitry.

3. PROGRAMMING LANGUAGES AND DOCUMENTA-TION

INTRODUCTION

- **3.01** The 1A ESS switch program is derived from two sources:
 - (a) Maintenance and administrative programs developed for the 1A processor
 - (b) New application programs developed expressly for the 1A ESS switch.
- **3.02** This part provides a brief introduction to the 1A processor and the 1A ESS switch program-

ming language and associated documentation. A description of the program development process is also provided.

MACHINE INSTRUCTIONS

3.03 Instructions to the 1A processor (machine instructions) must ultimately be represented in

binary. These instructions may be two 24-bit words or one 24-bit word. The primary factor which determines the length of an instruction is the number of bits needed to represent the data field and/or the number of options or additional actions which are encoded in the instruction.

3.04 Base cycle time of a particular instruction is the time required by the processor to carry out the functions specified by the instruction. The 1A processor is designed to execute instructions in fixed units of time referred to as processor cycles. ♦With the introduction of fast stores, most 1A instructions now execute within 700 nanoseconds, even if memory access is required.♥

ISS 3, AT&T 231-045-000



Fig. 4—Operation Circuitry

AT&T 231-045-000

1A PROCESSOR ASSEMBLY LANGUAGE

3.05 The machine instructions are generated by translation of a set of mnemonic instructions, designated as the 1A processor assembly language. This language is used by a programmer to transform the requirements of a program into the machine instructions required to execute the program. After a program is written in this language, it is input to an assembly program ♦which may or may not generate machine instructions, and if generated, may generate one or more machine instructions per source statement. ♦ A description of the assembly program and a brief discussion of the overall assembly process are given in paragraph 3.19.

3.06 In assembly language statements, the operation of each instruction is coded mnemonically and the data and instruction addresses are in symbolic form. For example, the mnemonic for the STORE instruction is simply S. An example is:

S X, SYMADDR

The data word to be stored is in register X and the address at which the word is to be stored is symbolically encoded as SYMADDR.

3.07 The 1A assembly language contains four classes of instructions. Each of these classes and the instructions which fall into each class are discussed in detail in section 254-280-020 (1A Processor Assembly Language). These classes are:

- (a) General processing instructions, which are for directing or controlling the 1A processor
- (b) Peripheral instructions, which transmit and receive data between the processor and the switching system
- (c) Maintenance instructions, used to test central control, memory, and the buses
- (d) Pseudo-operations, which are used only for certain directions to the assembler and loader programs in development of the overall program.

MACROS

3.08 Many similar functions are performed repetitively throughout the 1A processor and 1A ESS switch software programs. The programming of

Page 10

these functions is simplified by the use of the macros. A macro is a high-level statement which is translated by the assembly program into a predefined sequence of instructions or data. As an example, if the contents of a memory location (DATA_WORD20) needs to be added to the contents of another location (OTHER_ LOCATION) and the result stored in a new location (NEW_LOCATION), the entire operation could be performed by the following macro call:

ADD DATA_WORD20, OTHER_LOCATION RESULT=NEW_LOCATION REG=X

The following 1A assembly instructions (and machine instructions) would be generated by the assembly program:

- L X, DATA_WORD20 (Load contents of DATA_WORD20 in register X)
- A X, OTHER_LOCATION (Add contents of OTHER_LOCATION)
- S X, NEW_LOCATION (Store results in NEW_LOCATION)

If this macro was defined by a programmer for use in only one program, it is called a programmerdefined macro and its definition would appear in the program listing for that program. If the macro is used in more than one program, it is a system-defined macro and its definition is in Datapool, a public library listing (see Datapool, paragraph 3.16). The definition of a macro includes its name, function, format, explanation of parameters, and the program listing comments.

3.09 The macro in paragraph 3.08 is a simplified example. Generally, a greater number of options in parameters is available, which in turn provides more diversity in the code which is produced. Through this diversity, a macro's usefulness is extensive.

- **3.10** There are two types of macros which generate instructions.
 - (a) General purpose macro: A macro which generates instructions that perform a common data manipulation function, eg, IF and LET macros

ISS 3, AT&T 231-045-000

(b) Special purpose macro: A macro which generates a code that performs a specific function according to the hardware or software design of a system, eg, the PRINT, CIN (change in network), and CIC (change in circuit) macros of 1A ESS switch.

ESS SWITCH PROGRAMMING LANGUAGE (EPL)

3.11 The 1A assembly language was previously defined as a language used by the programmer (and assembly program) to transform program requirements into machine instructions. The ESS switch programming language (EPL) is a higher-level language, with statements closer to English language statements. As such, EPL statements may translate into several machine instructions, meaning that programming logic takes place on a higher level, compared to the assembly language where one machine instruction is generated for each assembly statement.

3.12 Programs may contain both EPL statements and assembly language statements intermixed. During assembly of the program:

- (1) An EPL compiler will transform the EPL statement to assembly language statements
- (2) The assembly program will then convert these to the binary encoded machine instructions.

DIAGNOSTIC LANGUAGE (DL-1)

3.13 DL-1 is a macro language that consists of many individual statements. When these DL-1 statements are assembled, the results are data table-driven diagnostic programs that direct diagnostic tests to be run on 1A processor equipment. The diagnostic programs that run on the 1A processor are, in general, based on repetitive execution of simple tests involving:

- (a) Setting a location to a known value
- (b) Reading the value of a location
- (c) Comparing the read results with an expected value.
- **3.14** Most programs repeat the same type of test hundreds of times in diagnosis of a particular unit. The program instructions required to perform

each diagnosis of a particular unit differ only in the location address and the data to be read or written. Instead of repeating these instructions for each and every test, the unique portions of each, ie, addresses, data, and expected results, are referred to as data tables. Only one set of instructions, called a task routine, is then provided in the program to execute all these types of tests.

3.15 The DL-1 macro language is used to generate these data tables. A DL-1 macro is a high-level statement which is expanded by the assembly program into a predefined data table format. In general, each DL-1 statement has an associated test routine. A more detailed description of DL-1 is available in section 254-280-040 (Diagnostic Language-DL-1 Description 1A Processor).

DATAPOOL

- 3.16 Definitions and descriptions of data and macros which are used in more than one program pident are not given in each program listing, but appear in library listings available to all programs. These listings are designated as Datapool. Datapool is subdivided into the following sections (libraries):
 - (a) Macro Library: Contains the macro definitions and all names made synonymous with macro names.
 - (b) Symbol Library: Contains all other symbol definitions. This is the larger of the two libraries.

3.17 The macro library contains definitions of macros that are needed by more than one program pident. Each macro definition is preceded by a description which includes:

- Macro name
- Macro function
- Format for calling the macro
- The macro parameters.

A cross-reference section is provided in the macro library, giving the page and line number of the macro in the listing.

AT&T 231-045-000

3.18 The symbol library of Datapool contains all the data definitions used by more than one pident in the generic program. The symbol library contains the following:

(a) Memory Allocation Section: ♦All symbols requiring memory allocation are defined in the memory allocation section, even those symbols which are used by only one pident.

(b) Symbol Layout Section: ♦Memory allocation is not repeated in the symbol layout section but other attributes may be added to some symbols defined in the memory allocation section.

(c) Cross-Reference Section: For each symbol, the cross-reference section of this library includes:

- (1) Address (in the case of a symbolic name) or the value (if a symbolic constant)
- (2) Type (item, block, or table, etc)
- (3) Attributes which define certain characteristics of a symbol, such as the number of bits in an item and its displacement in a word.

The symbol library also contains an equivalent crossreference section which is ordered numerically by the value assigned to a symbol. For a more detailed description of Datapool, see section 254-280-010 (Datapool Documents).

PROGRAM DEVELOPMENT PROCESS

The generic program for any ESS switch of-3.19 fice is developed remotely from the ESS switch office because these offices do not have the capability of assembling the generic programs. Figure 5 shows the generic program development process. The source language statements, eg, assembly statements, EPL, DL-1, and macros, form a source program which is not executable by the 1A processor. Operation codes and symbolic addresses must first be translated into binary code. This translation process is the function of the assembly/compiler program, designated as the Switching Assembly Program (SWAP). The input to SWAP consists of the source program and two sets of Datapool libraries: one set of libraries containing information for the particular ESS switch application for which the generic pro-

Page 12

gram is being developed, and one set of libraries containing data common to the 1A processor and independent of application.

3.20 The assembler translates the assembly language statements to machine instructions on

guage statements to machine instructions on a one-to-one basis. Macros and EPL statements are first converted to assembly language statements and then to machine instructions. The primary output of the assembler is the object program module containing the executable code. Another output of the assembler is the program listing. The object program module is then input to the 1A loader program which loads and links pidents of the program by assigning program store addresses and resolving all external pident references. Information from the Datapool libraries is also used by the 1A loader program to establish program addressing (relative, vector table, or absolute) links for transfer and data location.

3.21 Output from a 1A loader program includes the loader map, available in each ESS switch of-

fice, which is a table identifying the starting address of the pident, the pident name, and the ending address of the pident. The other output from the 1A loader program is the loader history which is the generic program information without the office dependent data, and is used as input to the output tape program to generate a loader output tape. The loader output tape contains the generic program information. A detailed description of the generic program development and installation is given in section 254-280-020 (1A Processor Assembly Language).

OFFICE DATA

3.22 The generic tape contains the operational pro-

grams and data which are the same in every office. In addition to the generic data, all officedependent data, unique in each office, must be developed and installed. Office data includes the engineered quantities of call registers, trunk registers, network memory, etc, as well as translation data, which primarily reflects the office equipage and connections in addition to trunks and routing.

3.23 For new central office installations, all office dependent data is developed by the Parameter Data Assembler (PDA) and the Translation Data Assembler (TDA). The PDA and TDA are off-line processing systems which compile office data required by the generic program. The PDA compiles office data such as the number of call registers.

ISS 3, AT&T 231-045-000



Fig. 5—Program Development Process

amount of duplicated and unduplicated call store, etc. The TDA compiles the translation data needed for a particular ESS switch office. The output of these assemblers is placed on tape for input to the 1A ESS switch memory. The translation data may be altered by the telephone company after original installation to reflect changes in line and trunk assignments as well as routing information via recent change inputs. However, the parameter data can only be altered by AT&T.

PROGRAM LISTING

3.24 A program listing is a hard copy record of a program which describes the objectives of the program, lists all instructions, and defines all data unique to the program. The listing is produced by the assembly program. Each program consists of one or more subunits called program identifications (pidents). There are two types of listings: the standard program listing and the diagnostic phase program listing. Diagnostic programs are divided into phases, where each phase contains a grouping of

tests. Each phase is designated as a pident. Although the formats of each type of listing are different, each is composed of five sections:

- Prologue Section
- Macro Definition Section
- Data Definition Section
- Program Section
- Cross-Reference Section.

In addition to a description of formats of each section, section 254-280-030 (Program Listing—Description) identifies standards which provide for detailed narrative information and comments in the listings to aid the reader in understanding the purpose, flow, and contents of each program.

AT&T 231-045-000

4. PROGRAM STRUCTURE OVERVIEW

GENERAL

The organization of the 1/1A ESS switches 4.01 program is strongly influenced by the fact that it must operate in real time. That is, the program must respond promptly to signals and data submitted to it by other switching systems and customers. In addition, it must respond quickly to errors detected by one of the many trouble detector circuits. These circuits are designed into the hardware to assure dependable operations within the system at all times. Whenever it fails to do so, the result may be improper handling of calls and a general degradation of service. For example, failure to detect digit signals may result in directing a call to a wrong number, or failure to outpulse digits to another office promptly will cause the other office to return overflow tone to the calling customer. Therefore, it is necessary to establish a hierarchy of program tasks. Some tasks must be performed on a strict schedule; others may be delayed without significant adverse effects.

INTERRUPT SYSTEM

4.02 The central processor has an interrupt mechanism within it which seizes control of the system momentarily when a system configuration, a fault detector, or testing of a processing type interrupt signal occurs. The interrupt system causes the central control to stop its present program task, stores the program address at which the interrupt occurred, and then transfers to the appropriate emergency action, fault recognition test, or clock-controlled input/output program. When the interrupt program task as interrupted or to a safe starting point in the maintenance program.

4.03 Figure 6 illustrates this overall plan. The interrupt sources and their associated programs are arranged in a hierarchy of ten interrupt levels. From highest to lowest, these levels are designated A, B, C, D, E, F, G, H, J, and K. The K-level interrupt is not used in the 1A ESS switch. An interrupt source assigned to a particular level can interrupt programs of lower level only, with the exception of the A and B levels which can interrupt each other as well as their own levels. The interrupt levels and their source conditions are listed in Table A.

Page 14

4.04 Every 5 milliseconds a system clock activates a level J interrupt which gives control to the input/output programs. The level H is used to interrupt the J-level input/output program when tasks being performed exceed 5 milliseconds.

INPUT/OUTPUT MAIN PROGRAM

A. Introduction

In order to perform all tasks promptly, the 4.05 individual task must not take too long. Thus it is necessary to limit the amount of processing performed by the interrupt programs. The input programs are confined to scanning for and recognizing input signals and storing the input information in a call store hopper. Each hopper is inspected by the base-level programs. When data is present in the hoppers, appropriate base-level programs start or continue the processing of the call. Likewise, call store buffers are provided for the base-level programs to load output area. At an appropriate time, the call store buffers are unloaded by output programs which deliver the information to the peripheral equipment. The peripheral order buffers are used to store address and control information for peripheral equipment, such as network controllers and signal distributors. These buffers provide the means for communication between the scheduled input/output programs and the base-level call processing programs. In a 1A ESS switch, flags are set in an activity word which is used in the base-level programs. This is described in paragraph 5.04.

4.06 The 700-nanosecond clock pulses in the central

control are counted, and every 5 milliseconds (actually 5.005) the counting circuit generates an output signal which interrupts the base-level program being performed. The interrupt signal causes the central processor to transfer to the J-level input/output main program. All input/output programs are classified into high-priority and low-priority tasks according to the frequency and urgency with which these tasks must be performed.

4.07 The low-priority tasks can be delayed for a few milliseconds without an adverse effect on the operation of the system. This will be the case when the coincidence of input work under a peak traffic load causes the system to take more than 5 milliseconds to complete the high- and low-priority tasks. In this event the H-level interrupt will occur and the low-priority work will be interrupted. The



ISS 3, AT&T 231-045-000

Fig. 6—Program Control Plan

accumulated high-priority work will again be performed before returning to the low-priority program that was interrupted.

B. Characteristics

4.08 Since this program must be executed every 5 milliseconds, the time required by the central control to cycle through all of the input/output task programs is held to a minimum, even at the expense

of a small increase in the total number of program words. For example, it is expedient in some cases to have a number of program blocks that perform nearly equal tasks instead of a common program capable of performing all of the tasks. A common program would, in general, involve more machine operations to accommodate the small variations in each of the individual programs and, as a result, would require more time.

AT&T 231-045-000

TABLE A

INTERRUPT LEVELS

LEVEL	SOURCE CONDITION	
Α	Manually Initiated	
В	Processor Configuration	
С	Central Control Mismatch	
D	Call Store Read/Write Failure Auxiliary Unit Read/Write Failure* Protected Area Violation* Pushdown Stack Violation*	
Е	Program Store Read/Write Failure	
F	Peripheral Unit Failure	
G	Maintenance Clock Time-Out Special Match Function Utility Computer	
Н	Interrupt J Level After 5 ms	
J	Interrupt Periodically After 5 ms	
К	Interject Time-Out†	

* Denotes 1A ESS switch only.† Not used by 1A ESS switch.

1 Not used by IA ESS switc

4.09 The program plan is sufficiently flexible that the same program can provide service after changes in the system due to growth. Also, the same program must operate during and after certain changes in the features offered by an office.

C. Organization

4.10 A block diagram of the input/output main program is shown in Fig. 7. At 5-millisecond intervals, a J-level interrupt normally occurs and control is transferred to the input/output main program, which operates as follows:

(a) It saves the contents of the central control registers to allow resumption of the base-level program at the point of interruption.

Page 16

(b) It updates the time counter and activates, one at a time, all input/output programs that require action. If a 5-millisecond interrupt occurs before the input/output programs are executed, an H-level interrupt occurs. Then the input/output tasks, which must be executed to ensure proper call processing, are executed.

(c) It then refills the central control registers with the information saved in (a) and returns control to the interrupted base-level program.

5. BASE-LEVEL PROGRAMS

GENERAL

5.01 The bulk of the 1/1A ESS switches programs, both call processing and maintenance, are executed on the base level (level L) without interrupt lev-



els A through K in effect. All base-level work can be deferred to some extent, but the amount of delay each program can tolerate varies widely. It is for this reason that a priority system implemented by a control program is used within the base level.

MAIN PROGRAM

5.02 All base level programs are controlled by a single program called the Executive Control Main Program (ECMP). In the 1ESS switch, the main program performs its control function on the base

ISS 3, AT&T 231-045-000

level with the use of six priority classes of programs. The highest priority class is called interject. The other five classes are A, B, C, D, and E, in descending order of frequency of examination. Specifically, the main program delivers control to these frequency classes according to the following pattern which is repeated endlessly:

...ABACABADABACABAEABACABADABACAB...

5.03 The 1A ESS switch has refined and enlarged the design of the base level programs. The new algorithm incorporates two major concepts. First, the base-level scheduling universe is expanded to include a domain external to the existing five frequency classes. Second, the idea of performing or looking for work only when it is "time to do so" is incorporated.

5.04 The base-level frequency classes are retained and remain internally intact from a functional viewpoint. However, the method of visiting the classes is changed. In general, base-level main program classes are scheduled by a J-level routine in pident ECIO, which is executed every 5 milliseconds.

6. ORGANIZATION OF 1/1A ESS SWITCHES SOFT-WARE SECTIONS

GENERAL

6.01 Figures and tables are referenced in this part which:

(a) Describe the organization and assignments of sections under the individual major system software functions.

(b) Provide pident section cross-references to facilitate access information on any function or individual program.

An explanation of each table and figure is given in the following paragraphs.

FUNCTIONAL ORGANIZATION OF 1/1A ESS SWITCHES SOFTWARE DESCRIPTIONS

6.02 The organizational chart in Fig. 8 illustrates the assignment of sections to major functions of the overall 1/1A ESS switches program structure.

AT&T 231-045-000

The four levels or groups of documents as shown in Fig. 8 are:

- System Level Description
- Major Control Level Descriptions
- Program Functional Descriptions
- 1A Processor Descriptions.

The first six digits of the section numbers have been assigned to show the breakout of the 1A processor, 1/1A ESS switches, and 1A ESS switch programs as follows:

NUMBER	DESCRIPTION			
231-045-	1/1A ESS Switches Program/ Documents			
231-310-	1A ESS Switch Programs/ Documents			
254-280-	1A Processor Program/ Documents			

The last three digits designate the functional portion on the organizational chart in Fig. 11 as follows:

NUMBER	DESCRIPTION
-0XX	Support Documents
-1XX	Operational Software Structure
-2XX	Maintenance Software Structure
-3XX	Interrupt Software Structure
-4XX	Feature Based Structure

DESCRIPTION OF CONTENTS-1/1A ESS SWITCHES SOFTWARE SECTIONS

- 6.03 Table B supplements the organizational chart in Fig. 8 by providing a brief description of:
 - (a) The major software functions covered in each program description section

(b) Contents of each section support document.

SECTION-TO-PIDENT CROSS-REFERENCE INDEX

6.04 Table C serves as a cross-reference index for

all 1/1A ESS switches software descriptions and the programs/pidents described in each. The programs and pidents listed in the table are not intended to represent a complete office generic listing, but only to include those which require description in accordance with the high-level functional nature of these documents.

PIDENT-TO-SECTION CROSS-REFERENCE INDEX

6.05 Table D provides a cross-reference index for all programs/pidents described in the 1/1A
ESS switches software descriptive documents. The programs and pidents listed in Table D do not represent a complete office generic listing, but only include those which require description in accordance with the high-level functional nature of these documents.

7. ABBREVIATIONS AND ACRONYMS

7.01 The following are abbreviations and acronyms used in this section.

DAR	Data Address Register
DL	Diagnostic Language
ECMP	Executive Control Main Program
EPL	ESS Switch Programming Lan- guage
PDA	Parameter Data Assembler
SWAP	Switching Assembly Program
TDA	Translation Data Assembler



AT&T 231-045-000



Page 20

∳fig. 8—Organization of 1/1A ESS Switches Software∉ (Sheet 2 of 4)

ISS 3, AT&T 231-045-000



Fig. 8—Organization of 1/1A ESS Switches Softwared (Sheet 3 of 4)

AT&T 231-045-000



ISS 3, AT&T 231-045-000

SECTION NO.		DESCRIPTION OF MAJOR CONTENTS
231-045-100	Operational Software	Describes three functions: call processing, equipment dependent overhead, and administrative work. All three are performed on both L (base) level and J level. Coverage also includes base level, J- and H-level interrupt structures, base level main program (including scheduling, timing, and system clock), J-level main program (including high-priority work and low-priority work), Automatic Overload Control (AOC), Line Load Control (LLC) maintenance, and emergency action recovery.
231-045-102	Supervision Modernization	Describes the Supervision Modernization feature for the 1 and 1A ESS switches and is a base feature in the 1E7, 1AE7 and later generic programs. The Supervision Modernization feature is part of a program modernization plan designed to aid in the development and testing of features for both the 1 and 1A ESS switches.
231-045-105	Call Processing — POTS	Describes programs which specialize in the processing of information associated with nonbusiness type calls. Coverage includes the following operations: dialing connection, digit analysis line, digit analysis trunks, ringing, and disconnect.
231-045-106	Call Processing — Centrex	Describes programs/subroutines used to process calls to and from a subscriber line located at a centralized telephone communication exchange. Coverage includes only those functions applicable to a centrex office.
231-045-110	Scanning	Describes a subsystem which supervises call processing activities by detecting and reporting changes of electrical states at specific points within the system. The scanning function detects change of states on lines, junctor circuits, trunk circuits, and selected other points for service requests, disconnects, and information such as line and trunk maintenance.
231-045-115	Outpulsing	Describes the outpulsing control program which includes interfacing with programs requiring outpulsing control, establishing necessary network connections, initializing the outpulsing control register, seizing the outgoing trunk, unloading the start-pulsing signal detection output link list, maintenance tests, and other outpulsing related functions.

Page 23

AT&T 231-045-000

TABLE B (Contd)

DESCRIPTION OF CONTENTS - 1/1A ESS SWITCHES SOFTWARE SECTIONS

SECTION NO.	TITLE	DESCRIPTION OF MAJOR CONTENTS
231-045-120	Peripheral Control	Describes the peripheral control programs used to interconnect line, trunks, service circuits, and tone sources associated with the central office. These programs perform specific functions (hunts for idle paths, administers network map, and administers path memory) associated with loading and unloading an instruction in a peripheral order buffer.
231-045-125	Operator Functions	Describes the operation programs which control calls to assistance operators, toll operators, information operators, business office operators, intercept operators, and repair service operators. Each program has its own functions and signaling arrangements which interface with other call processing programs.
231-045-130	Coin Functions	Describes the coin control program which handles toll calls, local calls, signaling, and detection of required operator signals for call originating from coin telephone sets.
231-045-135	Charging	Describes the charging programs which have responsibility for collecting, assembling, and storing data pertinent to billable calls (eg, message rate and toll calls). The Automatic Message Accounting (AMA) process is covered in this subsystem section.
231-045-140	Special Line Services	Describes the programs that allow the customer to have special line services. Speed calling, reverting calling, call waiting, call forwarding, add-on, and conference are examples of these special services.
231-045-145	Translations	Describes the translation program which consists of service routines which are used to transform known data supplied by a client program into related data that is returned to the requesting program. The translation program pro- vides client programs with related information about customer lines, directory numbers, trunk and service circuits, junctors office codes, rates, routes, and miscellaneous items.
231-045-150	Recent Changes	Describes the recent change subsystem which provides means for the telephone company personnel to alter translation data. Translation data is altered to reflect changing service require- ments of subscribers and internal system considerations such as growth, traffic engineering, network management, and more.

ISS 3, AT&T 231-045-000

TABLE	B	(Contd)

DESCRIPTION OF	CONTENTS —	1/1A	ESS	SWITCHES	SOFTWARE	SECTIONS
----------------	------------	------	-----	----------	----------	----------

SECTION NO.	TITLE	DESCRIPTION OF MAJOR CONTENTS
231-045-155	Queue and General Purpose	Describes queuing programs which act as administrators for various queues or lists containing items waiting to be handled by the system. This section also describes general purpose programs which perform preliminary work and particular functions for other client programs.
231-045-160	Toll/Tandem Switching	Describes programs required to establish connections necessary for toll/tandem service in 1/1A ESS switches. Toll/tandem offices provide switching capability for trunk-to-trunk connections.
231-045-165	Traffic Data Measurements	Describes traffic data measurement programs which are used to generate, accumulate, collect, and print out 1A ESS switch traffic data. This traffic data consists of peg, usage, and overflow counts generated by call processing and main- tenance programs as specific events occur.
231-045-170	Network Management	Describes network management programs which provide a means of reducing traffic overloads, resulting from earthquakes, snowstorms, telethons, etc. Network management closely interfaces with the Calling Line Identification (CLID) program.
231-045-175	Centrex Data Link Features	Describes data link features available to a centralized telephone exchange service that uses the data handling capabilities of a nearby 1/1A ESS switches central office. These features include calls handled by centrex attendant, transmission of lamp orders and reception of key signals, call pickup at night station, and answer codes from other noninward phones or premises.
231-045-180	Centrex Business Communication Services	Describes the essential operations for providing business communications services to centrex customers. The specific centrex operations described in this section include: (a) calling station identification, eg, centrex control unit originatins which require AMA or sampling; (b) record keeping for certain types of calls; (c) performing switching office functions in a tandem tie line network.
231-045-200	Maintenance Software	Provides an overall view of the maintenance software which can be divided into two areas: fault recognition/isolation and recovery.

AT&T 231-045-000

TABLE B (Contd)

DESCRIPTION OF CONTENTS — 1/1A ESS SWITCHES SOFTWARE SECTIONS

SECTION NO.	TITLE	DESCRIPTION OF MAJOR CONTENTS
231-045-200 (contd)		Fault recognition/isolation programs continuously exercise the system and isolate fault(s). The second area, recovery, provides programs which rapidly recover the call processing ability of the system during trouble conditions.
231-310-210	Fault Recognition	Describes the fault recognition program which is implemented by a central control interrupt circuit when a system fault (circuit troubles) is detected. The fault recognition program determines which system unit has failed and establishes an operational configuration.
231-045-215	Audit Programs	Describes the audit programs which consist of corrective programs that audit call store and program store for inconsistencies. Coverage includes error detection, writing corrective information into memory, initializing the system for the first time, audits used when changes are made to the system, and audits requested by TTY.
231-045-220	Peripheral Diagnostic and Exercise	Describes diagnostic programs which are used to localize fault(s) to a small number of plug-in circuit packs within a system unit that have been taken out of service. Exercise programs which closely interface with diagnostic programs to check for faults are also covered in this section.
231-045-225	Centrex and AIOD Diagnostic and Exercise	Describes programs designed to test the entire console data interchange system. Coverage includes the busying of faulty data links, testing the data link to isolate the fault, restoral and reinitialization to service of the repaired data link and certain centrex exercises.
231-045-230	Trunk and Service Circuit Maintenance	Describes the trunk and service circuit maintenance programs used for diagnostic testing on various trunks, junctors, and service circuits used in 1/1A ESS switches central office.
231-045-235	Trunk and Line Test	Describes the carrier group alarm program, the automatic line insulation test program, the incoming trunk test program, the automatic trunk test termination program, and the station ringer and touch-tone test programs.
231-310-240	Data Mapping	Describes data mapping which is used to copy transient data blocks from their current locations

ISS 3, AT&T 231-045-000

TARIE	R	(Contd)
ADLE	D	(Conta)

DESCRIPTION OF CONTENTS -	1/1A ESS SWITCHES SOFTWARE	SECTIONS
---------------------------	----------------------------	----------

SECTION NO.	TITLE	DESCRIPTION OF MAJOR CONTENTS
231-310-240 (contd)		to the locations which are compatible with the update issue of data.
231-045-245	System Performance	Describes program operations designed to indicate the system's ability to perform its call processing functions. These operations consist of tests which check various types of calls, queues, hoppers, registers, and special tasks.
231-310-250	Master Control Center (Man-Machine Interfacing)	Describes the Master Control Center (MCC) which serves as the interface between the switching system and operating telephone company personnel. It represents the central maintenance, control, and administration point of the 1A ESS switch.
231-045-255	Growth	Describes the growth programs which provide the required operations to change information about quantities of central office equipment as the office grows. Coverage also includes growth program operations during the cutover of a central office.
231-310-260	Local Utility	Describes the local utility program which provides the means to read, move, and, with certain restrictions, overwrite data retained in any addressable location in the system.
231-310-265	Input/Output Application Programs	Describes the TTY programs which serve as the input/output intermediaries between operating company personnel and 1/1A ESS switches programs.
231-045-270	Network Fabric Maintenance	Describes the network failure action program which is executed when the peripheral order buffer (POB) execution program encounters certain failing conditions during the execution of an order from a POB. Coverage also includes network fabric routines which serve primarily as an aid to maintenance personnel in testing, repairing, and replacing faulty crosspoints in the network fabric.
231-045-275	Ringing, Tone, and Recorded Announcement Maintenance	Describes the programs which monitor and test circuitry and equipment associated with ringing, tones, and recorded announcements.
231-310-280	Library Program Control	Discusses the concentration of all changeable information (ie, number of lines and trunks, types of signaling, and other variables) into one place.

AT&T 231-045-000

TABLE B (Contd)

DESCRIPTION OF CONTENTS — 1/1A ESS SWITCHES SOFTWARE SECTIONS

SECTION NO.	TITLE	DESCRIPTION OF MAJOR CONTENTS
231-310-280 (contd)		The programmed ability to interface with and tie off auxiliary programs (temporary loaded programs for growth and upgrading) are also covered.
231-310-300	Interrupt Recovery Software Control Structure	Provides an overview of the interrupt recovery software control structure that is entered after an interrupt has occurred. Coverage also includes description of the system interrupt recovery program, the A-level interrupt recovery program, and the restart program for all levels of interrupts.
231-310-310	System Reinitialization	Describes the programs that reinitialize the software system in the event of severe memory mutilation. These programs reinitialize program store, call store, and file store with tape- stored data.
231-310-320	Hardware Recovery	Describes the programs that are designed to recover the system processing ability when the fault recognition on software sanity programs are unable to process the given faults. These programs attempt to establish a valid hardware configuration for the processor and the periphery.
231-310-330	Software Initialization	Describes the program that executes any phases requested to accomplish a return to normal processing. A description of the program which guarantees that the hardware state of a line agrees with the software state of the line is also included.
231-310-340	Emergency Mode Control	Describes the program that provides an emergency method for the 1A ESS switch to return to an operational state. This program is only executed when a severe hardware or software malfunction prevents system recovery via the normal automatic or manual techniques.
231-045-405	Toll Common Channel Interoffice Signaling	Provides a functional description of the programs which comprise the Toll Common Channel Interoffice Signaling System.
231-045-410	Digital Carrier Trunk Software	Provides a software functional description of the operational, maintenance, and interface capabilities of the digital carrier trunk software.
231-045-415	10A Remote Switching System	Describes the call processing actions performed by the Remote Switching System Programs.

-

ISS 3, AT&T 231-045-000

TABLE B (Contd) #DESCRIPTION OF CONTENTS — 1/1A ESS SWITCHES SOFTWARE SECTIONS#		
SECTION NO.	TITLE	DESCRIPTION OF MAJOR CONTENTS
231-045-430	Peripheral Unit Controller	Describes the programs which form the software functional interface between the ESS switch processor and the peripheral unit controller.
231-045-440	Peripheral Unit Controller/Data Link	Describes the functional operation of the peripheral unit controller/data link (PUC/DL) software for processing the information received from and sent to the remote terminals via data links.
231-045-445	HILO 4-Wire Operation and Maintenance	Describes the HILO 4-wire operational and maintenance software programs. This feature is to provide two electrically independent trans- mission paths through the switching network for toll applications.
231-045-455	Electronic Tandem Switching	Describes the Electronic Tandem Switching (ETS) feature software package consisting of a group of programs which enable the 1/1A ESS switches to serve as a tandem office in a centrex network. It gives centrex customers additional flexibility by allowing them to control station features and routing of calls. It also provides information to the customer about the status of the network and the individual calls.
231-045-460	E911 Programs	Describes the E911 (enhanced 911) software programs collectively which perform the control functions necessary for E911 tandem offices to selectively route 911 calls originated from any station in their 911 service area to the correct primary public safety answering point (PSAP) and provide specific E911 feature services.
231-045-490	ACMOS Operational Software	Describes the Automatic Customer Message Outputting System (ACMOS) software which per- forms the control functions necessary for providing call data to customer owned and maintained hotel/motel property management computer systems. The 1/1A ESS switches supply the tele- phone service for the administrative and guest lines directly from the centrex office.

AT&T 231-045-000

TABLE B (Contd)

DESCRIPTION OF CONTENTS - 1/1A ESS SWITCHES SOFTWARE SECTIONS

SECTION NO.	TITLE	DESCRIPTION OF MAJOR CONTENTS
254-280-010	Datapool Documents — Description — 1A Processor	Describes types of information contained in Datapool documents (PK computer listings). A Datapool library (portion of Datapool) may be either a macros library (containing macro definitions) or a symbols library (containing data definitions) and may be either a common library (1A processor) or an application (toll unique).
254-280-020	1A Processor Assembly Language — Description	Describes the 1A processor assembly language, a set of mnemonic instructions used to generate the machine language that controls the ESS switches using a 1A processor.
254-280-030	Program Listing — Description — 1A Processor	Explains the format of program listings (PRs) and describes the information contained in these listings for both a standard program and a diagnostic phase program.
254-280-040	Diagnostic Language (DL-1) — Description — 1A Processor	Describes the basic structure of DL-1, a macro language used by diagnostic testing programs applicable to 1A processor equipment. Explains each DL-1 statement and provides examples.
254-280-110	File Store Administration Program — Description — 1A Processor	Describes the File Store Administration Program (DKAD) used to transfer information between (to or from) a file store (disk storage) and a client program.
254-280-111	Input/Output Programs — Description — 1A Processor	Describes the input/output (I/O) programs used to process input and output messages between a hardware terminal (TTY, CRT, etc) and a client program.
254-280-112	Auxiliary Data System Operational Programs — Description — 1A Processor	Describes the Data Unit Administration Program (DUAD), the Automatic Message Accounting Data Transfer Program (AMDX), and the backup Tape Writing Program (TWRP) and its control program (TWRT). DUAD administers the transfer of data between (to or from) tape storage and client program. AMDX and TWRP/TWRT are clients of DUAD. AMDX is primarily used for toll call billings; TWRP (a library program) writes the backup tapes used by system reinitialization and certain system audits.

ISS 3, AT&T 231-045-000

TABLE B (Contd)

DESCRIPTION OF CONTENTS - 1/1A ESS SWITCHES SOFTWARE SECTIONS

SECTION NO.	TITLE	DESCRIPTION OF MAJOR CONTENTS
254-280-210	Maintenance Control Program — Description — 1A Processor	Describes the common pidents of the Maintenance Control Program (MACP). MACP schedules and controls the execution of deferrable, base-level maintenance programs and utility programs. See section 231-045-200 for a description of the application MACP pidents.
254-280-211	Paging Program — Description — 1A Processor	Describes the Paging Program (PAGS) which supervises the retrieving of a program stored in file store and placing of this program in core store for execution.
254-280-212	Master Control Console Common Control and Monitor Program — Description —1A Processor	Describes the Master Control Console Common Control and Monitor program (MCCM) which controls input and output functions associated with the Master Control Console (MCC) common processor panels and power control switches on various processor units.
254-280-213	Library Control Program — Description — 1A Processor	Describes the Library Control Program (LIBR) which controls all library client programs. Library programs are special, infrequently used programs designed for running tests associated with installations, office growth, traffic, etc.
254-280-220	Diagnostic Programs — Description — 1A Processor	Describes the common diagnostic programs (ie, 1A processor diagnostic and the Diagnostic Control Program [DCONMAIN]). A diagnostic consists of a local control program which points to table-driven (segmented test phases) and to task subroutines for testing 1A processor units. DCONMAIN controls the execution of diagnostics.
254-280-230	Diagnostic Results Post- Processing Program — Description — 1A Processor	Describes the common portion of Diagnostic Results Post-Processing Program (DRPP). DRPP is a collection of common and application programs that are used to turn failing diagnostic raw data into a list of components that could possibly be faulty.
254-280-250	Generic Utility Program (GULP) — Description — 1A Processor	Describes GULP, a manually initiated program, which is used in performing utility functions, ie, dump, load, and copy, to aid in the resolution of hardware/software problems.

AT&T 231-045-000

TABLE B (Contd)

DESCRIPTION OF CONTENTS - 1/1A ESS SWITCHES SOFTWARE SECTIONS

SECTION NO.	TITLE	DESCRIPTION OF MAJOR CONTENTS
254-280-260	Audit Programs — Description — 1A Processor	Describes the 1A processor Writable Store Audit Program (SAWS), System Audit of Stores Using Tape programs (SAST), and Auxiliary Unit System Audit program (SADK). SAWS and SAST check the integrity of the stored program and nontransient data, provide error information, and provide corrective action. SADK initializes the file store system, audits memory, times file store requests, and audits AMA buffer points.
254-280-270	System Update Program — Description — 1A Processor	Describes the system update program which is used to load a complete generic program and/or office dependent data from tape into a presently operating 1A processor system.
254-280-310	Fault Recovery Programs — Description — 1A Processor	Describes the fault recovery programs which isolate faults in the 1A processor system or direct program control to the appropriate peripheral fault recovery program if a nonprocessor fault is indicated.
254-280-320	Error Analysis Program — Description — 1A Processor	Describes the 1A processor error analysis programs (ERIF, ERAP) which gather various data during a fault recovery process and during diagnostic and other maintenance actions, and processes this data for analysis and retrieval.

ISS 3, AT&T 231-045-000

♦TABLE C

SECTION-TO-PIDENT CROSS-REFERENCE (NOTE)

SECTION AND PIDENT	PIDENT NAME
231-045-100 AOVD1A00 ECIO1A00 ECMP1A00 LLOD1A00	Automatic Overload Control Executive Control Input Output Executive Control Main Program Line Load Control and Toll Network Protection
231-045-102 SASS1A00 SCJT1A00 SSCD1A00 SSCN1A00 SSDC1A00 SSPL1A00	System Audit, Supervisory Signaling Scanner J and T Bit Control Supervisory Signal Change Direction Supervisory Signal Control Supervisory Signal Delivery Supervisory Signaling Path Locator
231-045-105 CHGD1A00 DINT1A00 DISC1A00 DITS1A00 ICAL1A00 ICRV1A00 ISXS1A00 ORDL1A00 PSPD1A00 PSPD1A00 PSTP1A00 PSTP1A00 RING1A00 RING1A00 RVRC1A00 SUSC0000 YFTO1A00 YRGD1A00 YTTO1A00	Scan Point Change Director Dialing Connection Disconnect Program Time Scan Junior Register Processing Digital Analysis Trunks Digital Analysis Trunks — Revertive Step-by-Step Incoming Calls Digital Analysis Lines Permanent Signal — Partial Dial Permanent Signal and Partial Dial Timing Program Step-by-Step Timing Ringing and Answer Detection Special Ringing Revertive Pulse Generation (Digit Reception) Supervisory Scan Incoming Trunk to Busy — Overflow or Special Service Circuit Trunk Guard Timing Originating Line to Busy — Overflow or Special Service Circuit
231-045-106 CXDS1A00 CXIC1A00 CXOR1A00 CXYH1A00	Disconnect Program Digital Analysis Trunk Originating Digit Analysis for Centrex Seize and Release Routines and L, J, and T Bit Administration

Note: This table does not represent a program and pident listing for a complete office generic but lists only those programs and pidents that require description in accordance with the high-level functional nature of these sections.

AT&T 231-045-000

♦TABLE C\$ (Contd)

SECTION-TO-PIDENT CROSS-REFERENCE

SECTION AND PIDENT	PIDENT NAME
231-045-110 CCLT1A00 DITS1A00 MUMB1A00 OGGT0000 OGLF1A00 OGWN1A00 RSCN1A00 SURG1A00 SXS10000	Supervisory Scan Time Scan Junior Register Processing Program Multiple Bit Scan Revertive Pulse Detection Scanning Line Ferrod Scan Start Pulsing Signal Detection Program Digit Reception Scan Ring Trip Supervisory Scan Step-by-Step Incoming Dial Pulse Detection
231-045-115 DPGE1A00 DPOP1A00 MFOP1A00 MFPR1A00 MFTL1A00 OGGT0000 OGPC1A00 OGRV1A00 OGTC1A00 OPC1IA00 RVRC1A00	Dial Pulse Digit Generation Dial Pulse Outpulsing Control Program Multifrequency Digit Transmission Multifrequency Transmitting Control — Load Tones in MFJR Multifrequency Transmitting Control Revertive Digit Reception Panel Call Indicator Pulse Digit Generation Revertive Outpulsing Control Outpulsing Control Panel Call Indicator (PCI) Outpulsing Revertive Pulse Generation (Digit Reception)
231-045-120 CHAT1A00 CHT1A00 CICS1A00 DSUB1A00 JPOB1A00 NCIN1A00 NMAC1A00 NMAC1A00 NTWK1A00 NTWK1A00 QEPR1A00 QEXC1A00	Peripheral Order Load Program for Change in Circuit Peripheral Order Load Program for Change in Circuit Change In Circuit Subroutines Distributor and Scanner Subroutines J-Level Disconnect for Step-by-Step Incoming Trunk Change in Network Network Mapa Administration Network Map Administration Network Transition Control Program Network Path Hunt Peripheral Order Buffer Execution Program Peripheral Order Buffer Execution Program
231-045-125 OFGT1A00 OFML1A00 OFNT1A00 OFTR1A00 TSP51A00 231.045-130	Operator Functions — Miscellaneous Outgoing to Switchboards and Desk Emergency Manual Line Program Operator No-Test Toll Switch Recording Traffic Service Position System Programs
CNCR1A00 COCN1A00 COIN1A00 DCNT1A00 OFTR1A00	Coin Control for RSS Program Coin Control Coin Charging Dialing Connections Program Operator Functions Program

ISS 3, AT&T 231-045-000

TABLE C (Contd)

SECTION-TO-PIDENT CROSS-REFERENCE

SECTION AND PIDENT	PIDENT NAME
 231-045-135 AMAC1A00 CAMA1A00 CDIS1A00	Automatic Message Accounting Data Accumulator Centralized Automatic Message Accounting Centralized Automatic Message Accounting Disconnect
231-045-140 ADBN1A00 ADCI1A00 ADDA1A00	Multiport Control and Switching — Abandon and Answer Conference Register Initialization Multiport Control and Switching — Dialed Additions
ADDB1A00 ADDX1A00 ADDR1A00 ADPB1A00 ADPT1A00 ADUP1A00 ADUX1A00 CCAD1A00 CFUP1A00 TXFR1A00 WAIT1A00	Drop-Back Analysis Multiport Control and Switching — Dialed Additions for Centrex Multiport Control and Switching — Action Requiring Filtering Initial Peripheral Order Buffer Loading Program Tag Report Analysis Update Routines Multiport Control and Switching — Update Routines for Centrex Customer Changeable Speed Calling Call Forward Usage Print Call Forwarding Service Call Waiting Program
231-045-145 NEJR1A00 TRANCOMN TRBD1A00 TRB1A00 TRC1A00 TRC1A00 TRC1A00 TRL1A00 TRL1A00 TRU1A00 TVBD1A00 TVBD1A00 TVBD1A00 TVBD1A00 TVBD1A00 TVCD1A00 TVCD1A00	Junctor Translations Translation Program Translation Routines — Basic Digit Analysis and Conversion Translation Routines — Basic Line and Directory Number Translation Routines — Basic Trunk Translation Routines — Centrex Digit Analysis Translation Routines — Centrex Line and Directory Number Translation Routines — Centrex Trunk Translation Routines — Centrex Trunk Translation Routines — Line Cutover Translation Routines — Multiline Hunt Arrangements Translation Routines — Universal Subroutines Translation Data Verification Messages — Basic Digit Analysis Translation Data Verification Messages — Basic Line and Directory Number Translation Data Verification Messages — Basic Trunk Translation Data Verification Messages — Centrex Digit Analysis Translation Data Verification Messages — Centrex Line
231-045-150 QURC1A00 RCCH1A00 RCDY1A00 RCFI1A00 RCIB0000 RCIE1A00 RCIE1A00 RCIG1A00	Queuing for Recent Change Control Recent Change Change Control Delayed Storage and Activation Recent Change Format Interpreter Recent Change Interface Buffer Recent Change Input Editor Recent Change Input Editor
AT&T 231-045-000

♦TABLE C€ (Contd)

SECTION-TO-PIDENT CROSS-REFERENCE

SECTION AND PIDENT	PIDENT NAME
RCK11A00 RCMU0000 RCS11A00 RCTF1A00 RCTS1A00 RCVC1A00 RCWL1A00 RSUB1A00	Recent Change Keyword Input Recent Change Message Update Recent Change Shared Information and Table Subroutines Recent Change Translator Format Builder Recent Change Table Subroutines Recent Change Validity Check Recent Change Work List Processing Recent Change Subroutines
231-045-155 COPR1A00 CXYH1A00 QAPR1A00 QCDL1A00 QEDA1A00 QEDA1A00 QTAL1A00 QTAL1A00 QTAL1A00 QTAL1A00 TRCE1A00 WQUE1A00 YAHA1A00 YCLK1A00 YFDS1A00 YFT01A00 YFT01A00 ZER01A00	Report and Miscellaneous Subroutines Seize and Release Routines and L-, J-, and T-Bit Administration for Centrex QTL — Queue Administration and Processing QTL — Queuing Data Link ACD QTL — Customer Interface and Special Auditing Routines QTL — Queue Entry and Destination Assignment Routines QTL — Queue Entry and Destination Assignment Routines QTL — Queue State Information Features QTL — Audible, Disconnect, and Line Termination Routines QTL — Audible, Disconnect, and Line Termination Routines QTL — Queuing For WATS Call Trace Queue Administration Seize and Release Routines and L-, J-, and T-Bit Administration Register Linking Routine Scan of Single Master Scanner Point Incoming Trunk to Busy, Overflow, or Special Service Circuit Miscellaneous Register Subroutines and Tables Originating Line to Busy, Overflow, or Special Service Circuit Call Store Zeroing
231-045-160 TAND1A00 TOPR1A00 TSPS1A00	Tandem Connections Program Toll Operator Signaling Traffic Service Position System Program
231-045-165 PPMP1A00 TFCL1A00 TFPT1A00 TFPR1A00	Plant Measurements Program General Traffic Data Collection Traffic Data Printing Quarter Hour Traffic Data Collection
231-045-170 CLID1A00 EDAS1A00 EDVF1A00 NMEA1A00 NMGT1A00 NMIN1A00	Calling Line Identification List Administration EDAS Interface EDAS Translation Verification Routines EDAS/NM Interface Network Management Network Management Indicators

ISS 3, AT&T 231-045-000

TABLE C (Contd)

SECTION-TO-PIDENT CROSS-REFERENCE

SECTION AND PIDENT	PIDENT NAME
NMMP1A00 NMRR1A00 NMTC1A00 NMTD1A00 NMTG1A00	Network Management Maintenance Program Network Management Reroute Control Network Management Toll Code Blocking Transmit Dynamic Overload Control Signals Network Management
231-045-175 CNLP1A00 CXIO1A00 CXKY1A00 CXLO1A00 CXTA1A00	Centrex Console Lamp Control Program Centrex Input-Output Program Centrex Group Status Check, Block, Queue, Seize Console Register Line and Trunk Seizure of Centrex Attendant Trunk Answering Night Service
231-045-180 AIOD1A00 CXBV1A00 CXSF1A00 CXTP1A00 CX1X1A00 HMTL1A00	Automatic Identified Outward Dialing Busy Verify on Lines and Trunks Centrex Simulated Facilities Program Centrex Trunk Preemption Program 1XX Tandem Tie Line Program Hotel-Motel
231-045-200 CXMS1A00 DOCT1A00 MACAADMN MACR1A00 PAIRLOCL	Centrex Maintenance Supervisory Program Dictionary Trouble Number Production 1A ESS Switch Audit Scheduler Maintenance Control Program Processor/Application Interface Routines
231-310-210 AIFR1A00 CPFR1A00 NMRF1A00 SCFR1A00	Automatic Identified Outward Dialing Fault Recognition Central Pulse Distributor Fault Recognition Network Management Fault Recognition Program Scanner Fault Recognition Program
231-045-215 AUDSMDIO CXSR1A00 MACAADMN NEGN1A00 NMDT1A00 NSUP1A00 POMC1A00 SACT1A00 SACV1A00 SACX1A00 SADX1A00 SADA1A00 SADA1A00	Common Input/Output Audit Centrex Call Register Audit 1A ESS Switch Audit Scheduler Network Head Cell and Junctor List Audit Line Bit Audit Enable Maintenance Routines Peripheral Order Buffer Audit Cutover Program Receiver Scan Audit Centrex Registers Audit Regenerated Constant Audit System Audit Programs Hopper and Fixed Length Queue Audit

Page 37

AT&T 231-045-000

♦TABLE C(Contd)

SECTION-TO-PIDENT CROSS-REFERENCE

SECTION AND PIDENT	PIDENT NAME
SALTWORT SAMP1A00 SANK1A00 SAQU1A00 SARG1A00 SASU0000 SATS1A00 SAWSLOCL SURT1A00	Translation Audit Network and Map Audit Linkage Audit of Junior Registers Audit Variable Length Queues Call Register Audit Supervisory Scan Data Tables Audit Expanded Enable Audit Writable Store Audit Ring Tip Supervisory Scan Initialization
231-045-220 CPBD1A00 CPDG1A00 CPDX1A00 CPRX1A00 DCPBDGNC NMDP1A00 NMMX1A00 PUBD1A00 SCDG1A00 SCDX1A00 SCRX1A00	Enable and Verify Bus Diagnostics Central Pulse Distributor Diagnostics Central Pulse Distributor Exercises Central Pulse Distributor Routine Exercises Diagnostic Control for Peripheral Bus Network and Diagnostics Network Matrix Routine Exercises Peripheral Unit Bus Diagnostics and Exercises Scanner and Answer Bus Diagnostics Scanner Demand Exercises Scanner Routine Exercises
231-045-225 AIDG1A00 CXDX1A00 CXMA1A00 CXMC1A00 CXMC1A00 CXMS1A00	Automatic Identification Outward Dialing Central Data Link and Console Demand Exercise Program Centrex Maintenance Program Data Link Diagnostic Control Centrex Maintenance Supervisory Program
231-045-230 CXTN1A00 TERA1A00 TMAC1A00 TNDC1A00 TNDN1A00 TNKC1A00 TNLS1A00	Centrex Trunk Maintenance Diagnostic Program Trunk Error Analysis Program Trunk Maintenance Control Program Centralized Automatic Message Accounting Diagnostic Program Trunk Maintenance Diagnostic Program Trunk Maintenance Diagnostic Program Trunk and Service Circuit Maintenance Control Trunk List Programs
231-045-235 ALITI A00 APCII A00 ATTTI A00 CGTBI A00 ICALI A00 ITCII A00 ITTTI A00 LTDKI A00	Automatic Line Insulation Test ATMS Processor Controlled Interrogator Automatic Trunk Transmission Test Carrier Group Alarm, Trunk Make Busy Digit Analysis For Trunks CCIS Incoming Trunk Test Termination Incoming Trunk Test Termination Local Test Desk Program

ISS 3, AT&T 231-045-000

TABLE C (Contd)

SECTION-TO-PIDENT CROSS-REFERENCE

SECTION AND PIDENT	PIDENT NAME
MCCP1A00 ORDL1A00 PLUG1A00 PLIT1A00 RLTDK1A00 SRTT1A00 TBTF1A00 TLTA1A00 TLTA1A00 TLTC1A00 TLTC1A00 TLTD1A00 TLTD1A00 YFT01A00	Master Control Center Program Digit Analysis For Lines Plugging Up Remote Automatic Line Insulation Test Remote Local Test Desk Program Station Ringer Test Through Balance Test Facility Trunk and Line Test Panel Part A Trunk and Line Test Panel Part B Trunk and Line Test Panel Part C Trunk and Line Test Panel Part D Trunk and Line Test Panel Part E Incoming Trunk to Busy
231-310-240 DMAPAPPL	Data Mapping Control and Linking
231-045-245 DDD01A00 DTST1A00 LLOD1A00 RA DR1A00 SOBR1A00 SYPI	Direct Distance Dialing Service Observing Dial Tone Speed Test Line Load Control and Toll Network Protection Receiver Attachment Delay Report Program Multiline Service Observing System Performance Indicators
231-310-250 LTDK1A00 MALM1A00 MCCP1A00 MCCP1A00 MCTWADMN TLTA1A00 TLTB1A00 TLTB1A00 TLTD1A00 TLTD1A00 TLTE1A00	Local Test Desk System Alarm Maintenance Audit Maintenance Control Center Master Control Center Administration Trunk and Line Test Panel (A) Trunk and Line Test Panel (B) Trunk and Line Test Panel (C) Trunk and Line Test Panel (D) Trunk and Line Test Panel (E)
231-045-255 NETG1A00 SACT1A00	Network Make Busy Routine Cutover Program
231-310-260 LULPUTIL	Local Utility Program
231-310-265 IOCPIMC2 IOCPOMC2 IOCPOMT2 TTIA1A00	Input Message Directory and Catalog Output Message Catalog and Test Phrases Miscellaneous Input/Output Translation Routines TTY Input Message Directory and Catalog

AT&T 231-045-000

TABLE C (Contd)

SECTION-TO-PIDENT CROSS-REFERENCE

SECTION AND PIDENT	PIDENT NAME
TTOA1A00 TTOB1A00 TTOC1A00 TTOC1A00 TTOE1A00 TTOF1A00 TTOF1A00 TTOH1A00 TTOH1A00 TTOHA00 TTOLA00 TTOK1A00 TTOK1A00 TTON1A00 TTON1A00 TTON1A00 TTON1A00 TTOP1A00 TTPPIA00 TTPPIA00 TTWK1A00	TTY Output Message Catalog TTY Input Translation
231-045-270 NMFA1A00 NMFL2A00	Network Fabric Routines Network Failure Maintenance Action
231-045-275 RAMP11A00 TODA1A00 TOMK1A00	Recorded Announcement Machine Program Ringing and Tone Plant Diagnostics Ringing and Tone Plant Monitor and Exercises
231-310-280 PGID1A00	Generic Identification and Compatibility Tables
231-310-300 IREC1A00 MARP MARS MCAI SIRE	Interrupt Recovery Program 1A Processor Maintenance Restart Program 1A ESS Switch Maintenance Restart A-Level Interrupt System Interrupt Recovery
231-310-310 SYSRBASE SYSRCONT SYSRCSPS SYSRTPAD	System Reinitialization Base Recovery System Reinitialization Control System Reinitialization Call Store/Program Store Configuration System Reinitialization Tape Paging Administration
231-310-320 HARVRECV IOTWRECV PCRVCONT PCRVPUMP	Peripheral Hardware Initialization Input/Output System Restoration Routine Processor Configuration Recovery/Control Processor Configuration Recovery Pump from Disk

ISS 3, AT&T 231-045-000

TABLE C (Contd)

SECTION-TO-PIDENT CROSS-REFERENCE

SECTION AND PIDENT	PIDENT NAME
231-310-330 MIRVRECV NMLI1A00	Memory Integrity and Recovery Restore Cutoff Program
231-310-340 EMERRECV	Emergency Mode Control
231-045-405 C01C1A00 C02C1A00 C03C1A00 C03C1A00 C05C1A00 C05C1A00 C1AL1A00 C1CB1A00 C1CB1A00 C1CP1A00 C1CP1A00 C1CP1A00 C1CP1A00 C1OP1A00 C1OP1A00 C1OP1A00 C1OP1A00 C1OP1A00 C1OP1A00 C1OP1A00 C1PC1A00 C1PC1A00 C1TQ1A00	Incoming CCIS Trunk States Outgoing CCIS Trunk States CCIS-to-CCIS Trunk States CCIS-to-PTS Trunk States PTS to CCIS Trunk States CCIS Post ADC Failure Trunk States Alarms Change Back Common Change Over CCIS-to-PTS Routines CCIS Input Processing Link Security State Table Manual Actions Office Recovery CCIS Output Processor CCIS Output Processor CCIS Output Processor CCIS Office Recovery PTS-to-CCIS Routines CCIS-to-CCIS Routines CCIS-to-CCIS and Shared Administration Routines CCIS-to-CCIS and Shared Network Routines CCIS to-CCIS and Shared Network Routines CCIS Timing Routines Terminal Generic Program Terminal Generic Program Trunk Query CCIS Translation Integrity Check External Interface Routines Call Processing Audits
TAUP1A00	Data Terminal Frame Status Word and Enable Audit
231-045-410 DCTC1A00 DCT11A00 DCT01A00 DFMP1A00 TNTD1A00	DCT Change in Circuit DCT Frame Inpulsing DCT TTY I/O and Common Routines Facility Maintenance Control Combined Channel Unit Diagnostics

AT&T 231-045-000

♦TABLE C♥ (Contd)

SECTION-TO-PIDENT CROSS-REFERENCE

SECTION AND	
PIDENT	
231-045-415 DCNR1A00 RDIS1A00 RESW1A00 RMSG1A00 RNAD1A00	RSS Dialing Connection RSS Disconnect RSS Reswitch ROB Loading and Administration RSS Network Administration
ROBE1A00 ROBF1A00 RRTE1A00 RSUP1A00 RTAD1A00 RTRF1A00	ROB Execution ROB Failure RSS Message Routing RSS Supervision Report RSS Terminal Administration RSS Traffic
231-045-430 DIALIA00 DYLTIA00 PUCIIA00 PUCIA00 PUCRIA00 PUFRIA00 PUFRIA00 PUFSIA00 PUFSIA00 PUDAIA00 PUCAIA00 PUC2IA00 PUC2IA00 PUC2IA00 PUC2IA00 PUC2IA00 PUC2IA00 PUC2IA00 PUC2IA00 PUC2IA00 PUC3IA00 PUC7IA00 PUC7IA00 PUC7IA00 PUC8IA00 PUC8IA00 PUC1A00	Diagnostic Interpreter DIAL Phase Table PUC Initialization PUC I/O Control PUC Diagnostic Routines PUC Unloader PUC F-Level Recognition PUC F-Scan PUC F-Scan PUC Error Analysis PUC Error Analysis PUC State Control Module PUC State Control Module
231-045-440 PUDR1A00 PUDT1A00 PUID1A00 PUID1A00 PUTY1A00	PUC/DL Fault Recovery PUC/DL Tables PUC/DL Initialization PUC/DL TTY Interface

ISS 3, AT&T 231-045-000

♦TABLE C♥ (Contd)

SECTION-TO-PIDENT CROSS-REFERENCE

	SECTION AND PIDENT	PIDENT NAME
ł	231-045-445	
	ATTT1A00	Remote Office Test Line
	DCNT1A00	Dialing Connections
1	DPOP1A00	Dial Pulse Outpulsing Control Program
	HLCT1A00	HILO 4-Wire CSTI Tables
	HLDI1A00	Disconnect Action for HILO 4-Wire Switching
	HLIC1A00	Dialing Connection for 4-Wire Switching
	HLOP1A00	Outpulsing Actions for HILO 4-Wire Switching
	ICAL1A00	Digit Analysis Trunks
	ISXS1A00	Step-By-Step Incoming Calls
	ITCI1A00	CCIS Incoming Trunk Test Termination Program
	ITTT1A00	Incoming Trunk Test Terminations
	MFTL1A00	Multifrequency Transmitting Control
	OGTC1A00	Outgoing Call Control Program
	PMBT1A00	Precut Multifrequency Bylink Trunk
1	RADR1A00	Receiver Attachment Delay Report
	TAND1A00	Tandem Connect
	TBTF1A00	Through Balance Testing Facility
	TLTA1A00	Trunk and Line Test Panel Program Part A
	TLTB1A00	Trunk and Line Test Panel Program Part B
	TLTC1A00	Trunk and Line Test Panel Program Part C
	TLTD1A00	Trunk and Line Test Panel Program Part D
	TLTE1A00	Trunk and Line Test Panel Program Part E
	TNHC1A00	HILO CAMA Diagnostic Program
	TNHS1A00	HILO Service Circuit Diagnostic Program Part 1
	TNHT1A00	HILO Trunk Circuit Diagnostic Program
	TNHV1A00	HILO Service Circuit Diagnostic Program Part 2
	TNHW1A00	HILO Interprocessor Trunk Diagnostic
	WQUEIA00	Queue Administration
	231-045-455	
	ADDX1A00	Dialed Additions for Centrex
	AMAC1A00	AMA Data Accumulation
	CFGR1A00	Customer Facility Group Register Routines
	CGTB1A00	Carrier Group Alarm, Trunk Make Busy
	CHGD1A00	Scan Point Change Director
	CTRF1A00	Customer Traffic Data
	CX1X1A00	1XX Tandem Tie Line
	CXICIA00	Trunk Digit Analysis for Centrex Lines
	CXOR1A00	Originating Digit Analysis for Centrex
	DLUPIA00	ETS Dial-Up Data Line Control
	DPOPIA00	Dial Pulse Outpulsing Control
	ECAULA00	Distance Control and Status
L	ICALIA00	Ligit Analysis for Trunks

AT&T 231-045-000

♦TABLE C€ (Contd)

SECTION-TO-PIDENT CROSS-REFERENCE

SECTION AND	
PIDENT	PIDENT NAME
MDR01A00	Message Detail Record Output
NMTG1A00	Network Management Trunk Group Controls
ORLD1A00	Originating Digit Analysis for Lines
PTRF1A00	ETS Customer Pollable Traffic Data
PUIO1A00	PUC/DL Input/Output
QAPR1A00	Queue Administration and Processing
QCIA1A00	Queue Customer Interface and Audit
QEDA1A00	Queue Entry and Destination Assignment
QSIF1A00	Queue State Information Features
QTRK1A00	Terminate to Trunk Facilities
QWAT1A00	Queuing for WATS
RCCX1A00	Recent Change: Centrex Common Block
RCEI1A00	Recent Change: EPSCS Customer Common Block
RCFV1A00	Recent Change: Call Forwarding
RCLI1A00	Recent Change: Line Translations
RCRL1A00	Recent Change: Route List Routing
RCSF1A00	Recent Change: Simulated Facilities
RCTG1A00	Recent Change: Trunk Group
RCTS1A00	Recent Change: Recent Change Tables
RCUP1A00	Recent Change: Recent Change Update
RCXD1A00	Recent Change: Centrex Digit Interpretation
SAQU1A00	Variable Length Queue and Timing List Audit
SARG1A00	Call Register Audit
TAND1A00	Tandem Connections Program
TFCL1A00	Traffic Count Collection
TFQR1A00	Quarter-Hour Traffic Data
TRBD1A00	Basic Digit Analysis and Conversion
TRBL1A00	Basic Line and Directory Number
TRBT1A00	Basic Trunk Translations
TRCD1A00	Centrex Digit Analysis
TRCT1A00	Centrex Trunk
TTxx1A00	TTY Output Messages
TVBD1A00	Verify Basic Digit Analysis
TVBL1A00	Verify Basic Line and Directory Number
TXFR1A00	Temporary Transfer
YAHA1A00	Seize and Release Routines, L-, J-, and T-Bit Administration
231-045-460	
COPR1A00	Report and Miscellaneous Subroutines
CXDR1A00	Originating Digit Analysis for CTX
CXIC1A00	Trunk Digit Analysis
DCNT1A00	Dialing Connections/Check for Tandem or Dedicated E911 Trunks

ISS 3, AT&T 231-045-000

♦TABLE C€ (Contd)

SECTION-TO-PIDENT CROSS-REFERENCE

SECTION	
AND	
PIDENT	PIDENT NAME
DISC1A00	Disconnect Program
ESCA1A00	Call Administration and Translation Interfaces
ESMG1A00	Error Messages and Error Counts
ICAL1A00	Digit Analysis Trunks
ISXS1A00	Step-By-Step Incoming Calls
MFTL1A00	Multifrequency Transmitting Control
OGTC1A00	Outpulsing Control
RCEN1A00	Recent Change – Emergency Service Number E911
RCER1A00	Recent Change – E911 Selective Routing
RCES1A00	Recent Change – ESCO
SASF1A00	System Audit/Local Choke
TRBL1A00	Line and Directory Number Translations
TTIA1A00	TTY Input Messages
TTOI1A00	TTY Input Messages
TTOJ1A00	TTY Output Messages
TVBL1A00	Translation Verification Messages
TVMN1A00	Translation Verification Messages/Main Control Program
YAHA1A00	Seizure and Release of E911 Register, Check E911 Local Choke
231-045-490	
COPR1A00	Unlink Call Register
CXKY1A00	Routes Input Data Link Orders to the Routine that Processes ACMOS
	Error Messages
CXMC1A00	Maintenance Control for Data Link
CXMS1A00	Maintenance Control for Data Link
CXOR1A00	Give Busy Message
DLLD1A00	Buffer, Block Loading
HMTL1A00	Release Register No Overtime Charging (AMA)
IRAC1A00	Check for ACMOS Feature
IRBA1A00	Update DAG Headcell
ORDL1A00	Check ADD ON, Give Reorder
RING1A00	Send New I/O Messages on MLG Retry
SAID1A00	Builds (Audits) Call Store Output Buffers and Related Printers, and Verifies Integrity
SARG1A00	Audit Dump
TRBD1A00	Conversions
TRBL1A00	DN Centrex Translations
TRCD1A00	Centrex Access Code
TRML1A00	Fetch DLG, MLG, and Hunt List LEN Number
TVBL1A00	Verify
YAHA1A00	Fetch, Release OR
YTTO1A00	Apply Audible Supscan

Page 45

-

AT&T 231-045-000

SECTION-TO-PIDENT CROSS-REFERENCE

SECTION AND PIDENT	PIDENT NAME
254-280-110 DKAD	File Store Administration Program
254-280-111 IOCPIMC1 IOCPIMT1 IOCPINT1 IOCPINT1 IOCPPMD1 IOCPPMD1 IOCPPM21 IOCPPSC1 IOCPPSC1 IOCPOSC1 IOCPOMS1 IOCPOMS1 IOCPOMS1 IOCPOMT1 IOCPPCH1 IOCPPCH1 IOCPPCH1 IOCPPCH1 IOCPPCH1 IOCPPSUB1 IOCPSUB1 IOCPFIM1 IOCPFIM1 IOCPFIM1	IOCP Input Message Catalog IOCP Input Message Translator Routines IOCP Input Message Translator IOCP Input/Output Initialization Input/Output Unit Controller Protocol Handler External Routines Protocol Handler Input Routines Protocol Handler Input Routines Protocol Handler Recovery Routines Protocol Handler Scheduler IOCP Input/Output Handler IOCP Output Message Save and Retrieval IOCP Output Message Save and Retrieval IOCP Output Message Starter IOCP Output Message Starter IOCP Output Message Translator IOCP Output Message Translator IOCP Print Call Handler Protocol Handler Tables IOCP Channel Routine I/O Hardware Interface Subroutines IOCP Timing Client Service Routines Input Messages Catalog
254-280-112 AMDX DUAD DUAD01 DUAD02 DUAD03 DUAD04 DUAD05 TWRP TWRT	Automatic Message Accounting (AMA) Data Transfer Program Data Unit Administration Program DUAD Client Interface DUAD Command Dispenser DUAD TTY Input Message DUAD TTY Output Message DUAD Data Unit Controller Audit, Trouble Replacement, and Diagnostic Interface Backup Tape Writing Program (Paged) Backup Tape Writing Program (Core Resident)
MACP MACPAUD1 MACPGTIM	1A Processor Maintenance Control Program MACP Audit MACP G-Level Timing

ISS 3, AT&T 231-045-000

TABLE C (Contd)

SECTION-TO-PIDENT CROSS-REFERENCE

SECTION AND PIDENT	PIDENT NAME
MACPJCT1 MACPJSH1 MACPRJOB MACPROUT MIRA	MACP Job Control MACP Job Scheduler MACP Request Job Routines MACP Service Routines Manual Input Request Administration Program
254-280-211 PAGS PAGSUPER	Paging Program PAGS Supervisor
254-280-212 MCCM MCCMEPS1 MCCMSPS0	Master Control Console Common Control and Monitor Program MCCM Program Store 1 MCCM Program Store 0
254-280-213 LIBR LIBRABRT LIBREXER LIBRINPT LIBRLOAD LIBRLVT1 LIBRSTOP LIBRTRP1	Library Control Program LIBR Abortion of Library System (Interrupt Monitoring) LIBR System Exerciser LIBR Input Data Handler LIBR Load Library System From Tape LIBR Common Library Vector Table (1A Processor) LIBR Library System Terminator LIBR Common Traps Administrator (1A Processor)
254-280-220 ABDG00 ADDG00 CCDG00 DCON DCONMAIN DCONTABL FSDG00 IODG00 MBDG00 MCDG00 MUDG00 PDDG00	Auxiliary Bus Diagnostic Control Program Auxiliary Data System Diagnostic Control Program Central Control Diagnostic Control Program Diagnostic Control Program DCON (1A Processor Application) DCON Data Table File Store Diagnostic Control Program Input/Output Diagnostic Control Program Memory Bus Diagnostic Control Program Master Control Console Diagnostic Control Program Memory Unit Diagnostic Control Program Power Distribution Diagnostic Control Program
254-280-230 DRPP DRPPASUB DRPPCC DRPPDUS	Diagnostic Results Post-Processing Program DRPP Common Subroutines (Utility, Raw Data) DRPP for Central Control DRPP for Data Unit Selector

AT&T 231-045-000

TABLE C (Contd)

SECTION-TO-PIDENT CROSS-REFERENCE

SECTION AND PIDENT	PIDENT NAME
DRPPFS DRPPIO DRPPMC DRPPMU DRPPSSUB DRPSUPR	DRPP for File Store DRPP for Input/Output DRPP for Master Control Console DRPP for Memory Unit DRPP Common Subroutines (Tape Access, Summary Processor) DRPP Control Routines (Core Resident)
254-280-250 GULP GULPIMMD GULPUTPP GULPUTXP GULRUTCR	Generic Utility Program GULP Paged Immediate Verb Execution GULP Paged Message Processor GULP Paged Delayed Verb Execution GULP Resident Control
254-280-260 SADK SASR SAST SAWS SAWSBASE SAWSCMMN SAWSSUBR	System Audit for File Store (Disk) Administration Program System Audit of Stores Using Tape (Resident Portion) System Audit of Stores Using Tape (Paged) Writable Store Audit Program (1A Processor) SAWS Common Audit Functions SAWS Common Audit Functions SAWS Client Service Subroutines
254-280-270 SUAP1A00 SUFA1A00 SUPL1A00 SYUP SYUR SYUR SYURPS20	System Update for APS System Update for File Store for APS System Update Program System Update Program (Paged) System Update Program (Resident) System Update Program Store 20 (Resident Control)
254-280-310 APFRILEV APMHCNTL APFRICON APFRBASE AUFR AUFRCNTL AUFRCPGM AUFRCPGM AUFRDFOR AUFRTEST CCFR CCFRMAIN	APFR Interrupt Level AP Message Handler Controller APFR Interrupt Control APFR Base Level 1A Processor Auxiliary Unit Fault Recovery Program AUFR Control (Program Store) AUFR Call Store Program AUFR Deferred Fault Recovery (Program Store) AUFR Interrupt Level AUFR Test Routines (Program Store) Central Control Fault Recovery Program CCFR Main Control

ISS 3, AT&T 231-045-000

TABLE C (Contd)

SECTION-TO-PIDENT CROSS-REFERENCE

SECTION AND PIDENT	PIDENT NAME
CCFRTEST	CCFR Tests
CSFR	Call Store Fault Recovery Program
CSFRBASE	CSFR Code Essential to System Recovery Programs
CSFRNORM	CSFR Other System Recovery Program Code Including D-Level and Noninterrupt
DUID	Recovery Routines
DUFR	Duta Unit Fault Recovery Program
DUFRDFUR	DUFR Deterred Test Control Routines
DUFROFLN	DUFR Off-Line Routines
DUFRPCAU	DUFR Common Auxiliary Unit Service Routines
DUFRPCDU	DUFR Data Unit Selector/Data Unit Controller Software Removal/Restoral
20110000	Routines
DUFRPCSB	DUFR Base Subroutines
DUFRSUBR	DUFR Nonbase Subroutines
DUFRTADM	DUFR Test Administration
DUFRTSTS	DUFR Test Routines
DUFRTTYI	DUFR TTY Interface Routines
FSFR	File Store Fault Recovery Program
FSFRDGN	FSFR Diagnostic Interfaces
FSFRDISK	FSFR Stop and Start Routines; Initialize and Restore File Store for and From
DODOTAT	Maintenance Fump; System Opdate Routines
FSFRSIAI	Short-Term Error Analysis Subroutines
PFLR	1A Processor F-Level Fault Recovery Program
PFLRPIIR	Common System's Perinheral Unit (PU) F-Level Filter F-Level Fault
	Recovery for Master Control Console (MCC) and Input/Output
	Unit (IOU), Input/Output Processor (IOP), and Short-Term
	Error Analysis
PFLRBLMH	Base-Level Fault Recovery for IOU
PFLRDGNH	Base-Level Diagnostic Request Handler
PFLRRRCR	Collection of Subroutines for Use By PFLR and Other Maintenance Programs
	to Performs to Perform Diagnostic, Test, and Service Routines for
	MCC and IOU
PFLR PUMP	PUMP RAM Program to IOMP
PSFR	Program Store Fault Recovery Program DSED Call Store Cade for Use During F. Level Internunt and When Called by DCDV
DEEDDEDC	PSFR Call Store Code for Use During E-Level Interrupt and when Caned by FCRV
IOPUMPPC	DDCMP RAM Program for PC
IOPUMPRX	BX 25 RAM Program for PC
	DALO MANI FIOGRANI IO FO
254-280-320	
ERAP	1A Processor Error Analysis
ERIF	1A Processor Error Analysis Interface

Portable Video Camera Viewer

You've just got done installing a covert video surveillance system inside a Mosque. You only have a few minutes before the bad guys come back. You need a way to quickly verify the integrity of the camera's video output without any hassles... A perfect tool for that job is a GBPPR Portable Video Camera Viewer...

Overview

This is a very simple device to view the video output signal from any camera installation. The portable, hand-held monitor is made from the eyepiece of an old, clunky, 1980s-style camcorder. These eyepieces contain a miniature Cathode Ray Tube (CRT), which is just like little a television. The input signal to the controller for this eyepiece is the standard NTSC composite video signal, so there is no need to perform any fancy video signal conversions, at least on this model. The eyepiece can be powered from a standard, alkaline 9-volt battery. This little hack is so easy that even Emmanuel Goldstein couldn't fuck it up! Oh... Wait... Nevermind.

Construction & Pictures



Monitor eyepiece from an old RCA CMR300 VHS camcorder. It's actually a miniature CRT feeding a mirror set at an angle. The original video input comes in from the cable on the right. The connector with the red circle is the one we are interested in. Viewing the wires, from left-to-right, the YELLOW wire is for the **RECORD LED** (and can be cut off), the **ORANGE** wire is +9 VDC, with a current draw of around 120 mA, the **RED** wire is the **VIDEO INPUT**, and the **BROWN** wire is a common **GROUND**.



Alternate wire bundle view. The shielded wire (on the left) going into the 1/8–inch jack is for the microphone.



Test setup. A small CMOS camera (the black, square thing) is connected directly to the video input line. (YELLOW wire from the camera, **BLACK** wire is ground). +9 VDC is feeding both the camera and the eyepiece (**RED** alligator clips).



Eyepiece showing the video output from the camera. Add a few high–power infrared LEDs, and you'll have a cheap night vision viewer.



Putting everything back together. The original 1/8–inch jack for the microphone will become the new video input jack. Unsolder all the wires from the little support board, and "pin–out" the 1/8–inch jack's connections using a continuity tester. Then, prepare the wiring bundle for installation (top).



Installation of the new 1/8–inch video input jack. The **RED** wire goes to the corresponding **TIP** connection and the **BROWN** wire goes to the **SHIELD** and a common ground. The top cover is prepared with the installation of the 9–volt battery holder. The **ORANGE** wire will go to the battery holder's **POSITIVE** (+) terminal. The battery holder's **NEGATIVE** (–) terminal will be connected to common ground with a jumper wire. There is no need to wire in a switch, but it could be useful.



Close up picture of the microphone input jack converted into a video input jack.



Everything is put back together. A 1/8–inch mono plug to phono jack adapter may be needed, depending on your camera's output connection. Package the GBPPR Video Camera Viewer with a wide selection of different adapters and extra 9–volt batteries. Note the **CONTRAST**, **BRIGHTNESS**, and **FOCUS** adjustment potentiometers. Your eyepiece will most likely require readjustment. You'll have to do this via trial–and–error.



And it works! A few turns of electrical tape keep the eyepiece's viewer hood from rotating or breaking off.

The eyepiece's 120 mA current draw is about *twice* what a standard, alkaline 9–volt battery is capable of sourcing, so it doesn't last very long. About 15 minutes of continuous operation can be expected.

Micky "Cheesebox" Callahan

From http://www.spybusters.com/History_1958_Cheesebox.html

I thought this was interesting, as I've never seen it mentioned anywhere. Yes, everything you've read in \$2600 Magazine and learned at HOPE is wrong. There's a shocker!





Mickey "Cheesebox" Callahan has built bugging devices for Al Capone, Lucky Luciano and legitimate business. He invented this telephone switching device-originally housed in a cheesebox-to help bookies "lose" the police by transferring the call to an unknown number.

Micky "Cheesebox" Callahan – King of the Underworld's Wiremen

"Gerard Callahan, Sr., is a notorious criminal and has been highly publicized as the electronics expert of the underworld..."

"Cheesebox Callahan received his nickname from his innovative ability in maneuvering telephone wires and equipment used for bookmaking calls. A "cheesebox" is a device whereby when a telephone number is called, it is in fact picked up at another location so that the police are thwarted in detecting the recipient of a phone call."

-- Thomas J. Mackell, District Attorney, Queens County, New York.

Excerpt from: Cheesebox, Paul S. Meskil with Gerard M. Callahan, 1974 Prentice-Hall, Inc.

These words in a brief filed with the Appellate Division of the New York Supreme Court, express one opinion of Cheesebox Callahan. The description is accurate, but the man described is more complex than these words imply.

Cheesebox is a tough, sly, humorous little man who looks and talks as though he had been invented by Damon Runyon. He cheerfully admits to being a conniver, a crook and a cheat, but since he has almost never willingly participated in any violent, or even very vicious crime, he lacks the sinister grandeur of some of the big-time mafiosi. On might be tempted to think of him as a real-life equivalent of some minor character in Guys and Dolls.



But that would be unjust – Cheesebox Callahan is, in fact, a kind of genius. For nearly half a century he has been the acknowledged king of the "wiremen" – the electronic wizards of the underworld. His expert talents have been employed by the Mafia, the police, well–known businessmen and – possibly – even by a President of the United States. (Not, as it happens, Richard Nixon: Cheesebox says contemptuously that if he, rather than the "Whitehouse Plumbers," had been given the Watergate job, there never would have been a scandal.) Above all, Cheesebox's talents have been applied – sometimes appallingly, sometimes hilariously – to the illicit lining of his own pockets.

Given a different background, other influences, a different set of experiences, Cheesebox might now be a respected inventor or a famous scientist. Instead, the circumstances of his early life impelled him relentlessly toward a life outside the law. This is not said to excuse him; others have successfully overcome far greater environmental handicaps. But there is about his story an undeniable sense of waste, of great gifts irretrievably lost – both to Cheesebox and to the world at large. By the time Cheesebox first began to think seriously about going straight, he was already too deeply involved in crime. There were too many powerful people on both sides of the law who had lively personal stakes in keeping Cheesebox just as he was. Until recently Cheesebox was never able to muster the willpower to resist for very long either the pressures or temptations that kept him a crook.

But for the past several years he has been making a valiant effort to reform. Valiant is probably the right word, since some of the counterpressures are, quite literally, lethal.

. SUNDAY, So . . hibaR Cheesebox Callahan Goes Straight in Queens

By DAVID BURNHAM

Chresebox, a small es-hment in a quietly re-able sertion of Flushing, ts, is not a gournet food

tead, according to the

niced. nice was called a to because it looked and Callahan pot his from it. Callahan i during a recent in-



"A bookie rented a room atjushere in the city and the phone company to install two phones in it. He told his customers to call one of the shoars. The books called

ter kiz-a week froita that during 1960, ha year, 50 of his cheeseboner all over New York. The last time he was a sted. Callabas recaller he made the mi be made the mi

when he made the mis of hooking up one o evices as a special fa or one of his customers the time, to make tem tn," a captain w a trom into

and he kept pro if I would give up (ted cops I knew d let me go. But in't go for the deal a

in's specialty

track in Florida betting parlor.

en fra

d, he s

to the explanation of the diagram

"They were about to me when I convinced I was a friend of Lu-by giving them the fir-pic of numbers of h wate telephone num-

A Stint at Xavie

With this money, Call called his mother was

than did indeed grat rom Xavier in 1927. For Callaban, who

lived and worked in Qu since the late nineteen.

of his latest

If he succeeds, he will have reformed without repenting. He was what he was, and it is too late to apologize. Certainly he was "a notorious criminal," and there is no way that his crimes can be minimized or cosmetized. If he is to repay a debt to society, it can only be done in more practical ways - for example, by alerting honest people to the dangers of electronic surveillance, by instructing them in techniques for fighting it, and where necessary, by providing them with sophisticated, specially designed hardware to make the fight more effective.

He is doing these things and some other, more dangerous things, besides. So perhaps, in some measure, he will succeed in compensating for the old life. But he will never deny it existed. He was the best in his business, and he cannot help but take a kind of rueful pride in the fact. For quite a while he was the top man on the telephone pole.

How to Defend Yourself Against Bugging

The citizens of our country are on a fright kick. So much has been written in newspapers and magazines about bugging that many people are afraid to use their phones. All this has created a gigantic market for eavesdropping devices. The fakers who manufacture, advertise and sell these so-called listening devices are a bunch of parasites who palm off a lot of dime-store gadgets that perform haphazardly. These fakers are breaking the buyers as well as the law.

The law, by the way, is the Omnibus Crime Control and Safe Street Act of 1968, Title 3, Chapter 2512. It was supposed to protect citizens, but it has been undermined by so many crooks on both sides of the law hat it is now almost worthless. Politicians go on shouting for more protection on the streets, but what about protection for homes and businesses? I personally gave a plan to the late Robert Kennedy that could have been a remedy to invasions of privacy on telephones. That was years ago.

As far as most of the fancy bugging devices now on the market are concerned, really professional wiremen – that doesn't include the cops – wouldn't touch them. They don't need to. It's know-how, not gadgets, that makes a top wireman.

There are only maybe four or five wiremen in this country, and maybe four in Toronto, who are the real pros. They are all expert burglars, and when they decide to do a job on you, they don't have any trouble breaking into your house or office. They can disable any burglar alarm system ever made (except a team of attack dogs), and once they are in, they don't mess around with dime-store gadgets. They just make a few simple adjustments in the transmitter circuit of your telephone so that the mouthpiece becomes "live." This means that your phone is not only tapped for incoming and outgoing calls, but it is also acting like a microphone that picks up any conversation carried on in its vicinity.

Of course, these pros don't even have to enter your premises to put their work on. They know how to operate on both fused and nonfused cross-connection terminal boxes, on drop cable pole-mounted distribution terminal boxes, on stand-mounted distribution terminal plastic cable boxes, and so on and on. They also know how to get all the special information they need out of the Cable Record Office. If you are a layman, probably none of this means much to you, but you can bet they know what it means.



There isn't much you can do to prevent a real pro from tapping your phones, but fortunately there isn't much likelihood you will ever have to contend with one of the experts. If anyone did decide to tap your phones, he'd probably send along a couple of clowns who wouldn't even dare to climb a pole to bridge a crossbox.

Say the victim lives in an apartment. The clowns' usual M.O. would be to get hold of the apartment-house super. They story him about how they are "special" investigators and have information that the tenant in 3A is engaged in subversive activities and is a menace to the country. The super eats it up, along with the fifty they slip him, and takes them to the house crossbox.

Since all the other wires in the box are black, you can make book they will string a pair of brand-new white wires. Even though 3A is plainly marked on the terminals, they will louse up at least three other phones in the building. It will take the boys three hours to complete their work, even though Hathaway's Chimps could have done the job in thirty minutes.

Since by now the tenant in 3A will have figured out what's going on, he will probably begin his counter-attack by taking his phone off the hook and leaving it off all night long. This will automatically activate the boys' tape recorder and use up all their tape long before dawn. Alternatively, or as a second ploy, he can go down to the cellar after the boys have left, take the white leads off his pair of terminals and hook them to the pair belonging to the German couple who live in 6B. Finally, and probably best, he can take a short vacation in Miami.

All I am trying to do by telling you this story is to reassure you that if you have reason to think some "expert" is trying to bug your home or place of business, the chances are he won't know much more about bugging than you do. There are many things you can do to protect yourself. Here are some of them.

You should not have an outside cleaning agency service to do your office chores: They are easy for a "plant" to infiltrate. You should never allow a telephone man to enter your home or office without carefully checking his credentials. Before allowing him to touch your phone or wiring, you should check with the repair service (611) and if you think a bug has been placed, don't hesitate to call (on an outside phone) the phone company security office.

In dealing with the security office, there are a few things to bear in mind. Always get the name of the person you are speaking to. If the company says they have "tested" your line and that "there is no illegal tap on your phone," be sure to ask whether there is any tap on your phone, illegal or legal. If their answer is to start double-talking you, you can be pretty sure there is a tap.

That is the time to begin writing (certified mail, return receipt requested) to your local U.S. District Attorney, the Frankie Browns, your congressman, the Public Service Commission, the local newspaper and anyone else in authority you can think of. Even authorized wiretappers usually can't stand that kind of public static.

One way to protect your phone (I mean the instrument itself; there isn't much you can do to protect the wiring) is to seal on the screw caps of both the mouthpiece and receiver with any strong adhesive spray such as 3M Brand #77. If this has been done, anyone trying to get at the receiver or transmitter elements in your phone will at least have to break the seal and may wind up breaking the whole handset casing. You can do the same thing to the base: While the handset is off the cradle, turn the base upside down, remove the two threaded screws from the bottom, coat them with "liquid steel" and screw them back in as tightly as possible.

If you think your premises have been bugged, you should obviously go over all your telephone wiring, from the building crossbox (if there is one), to the block screwed to the wall in your room, to the instrument itself. In checking for non-telephonic bugs, you will probably have to move all the furniture and lamps and check the bottoms of everything, as well as base sockets, light switches and any other place some creep might hid his work. Follow any wires you don't recognize to their source and do what is necessary if that source isn't legit.

If you find a bug on your phone, immediately loosen a wire. If you find a transmitter planted anywhere, take a straight pin and puncture the diaphragm of the microphone. This will produce a transmitted sound so distorted that your words will sound like someone speaking Chinese through a mouthful of marbles.

But these are only verifications and temporary remedies. The really important thing to do, as I've said, is to notify the phone company, the cops, the FBI and everyone else as soon and as noisily as you can. If you were me, you would probably also get a couple of baseball bats and wait around in the dark to see if you could get a shot at the creeps when they come back to look at their work. But this I don't necessarily recommend.



Using the Alternative Enhanced Redirect Service Data Validation Tool

Overview

AT&T's Alternative Enhanced Redirect Service (AERS) is intended to support the business continuity processes of customer name-to-location by permitting alternate routing of incoming calls for existing AT&T Prime (Local) Services at sites that may be experiencing a temporary or permanent building, communication facility, system emergency, or T1 failure. The **AERS Data Validation Tool** checks defined parameters from the customer's AERS spreadsheet prior to loading and building the customer routing database in the Integrated Service Control Point (ISCP). This document will provide instructions for using the **AERS Data Validation Tool**.

Business Rules

- The AERS Data Validation Tool can be accessed using Microsoft Internet Explorer 5.0 or higher and is located at the following URL: http://He.Really.Does.Touch.Little.Boys.com/aers
- A customer group is simply a list of incoming telephone numbers that will be included on the spreadsheet sent to provisioning. A customer group using AERS has nine redirect options. The first option enables the customer to designate select incoming Telephone Numbers (TN) for redirection consideration. Options two through nine are available for the customer to create up to eight redirect options for each TN per customer group.
- The customer group AERS spreadsheet (which *must* be in a text format) sent to provisioning will have the following tabs:
 - Customer Group = 10 digit redirect TNs with no hyphens, dashes, etc.
 - Option Level = Contains the Carrier Identification Code (CIC) and Billing TN (BTN).
 - Group Info = Summary of group selections including passwords.
 - Control Numbers = TNs used to activate/deactivate AERS.
 - Security = Contact name information.
 - ◆ Maintenance = Construction Maintenance Center (CMC) contact number.
 - **Contract Price** = Pricing information.
- The **AERS Error Report** from the **Data Validation Tool** provides sales information on what needs to be validated or corrected on the AERS customer group spreadsheet. If any information within the spreadsheet is incomplete or incorrectly populated, the **AERS Web Tool** should identify the error so the sales team can review the data and resubmit the corrected information.

Using the AERS Data Validation Tool

Logging into AERS

- 1. You must use Microsoft Internet Explorer 5.0 or higher to access AERS at the following URL: http://He.Really.Does.Touch.Little.Boys.com/aers
- 2. Type in your Human Resources ID (HRID).
- 3. Type in your initial password of: ******
- 4. At the Welcome Screen, you can change you password if desired.

Note: The password will expire every *30 days*, regardless of use, on the last Monday of every month. The tool will allow you to change your password after the expiration. If your password expires and you still cannot update it, click on the *Reset Password* link. This will set the password to "*****" and an email will be sent to you confirming the password was reset. If you continue to have problems contact the system administrator for assistance.

5. Once logged in, you will select **AERS Provisioning Page** for importing the data or the **AERS Sales Page** to view the data and reports.

Version 1.0.6	AT&T L ^{Star} AERS (Alternate Enh	OCAL PROVISIONING t your net.working anced Redirect Solution	ıs) Login Page
	Welcome	, Please choose a page	to visit
	HF 6 Pas Co	ID word firm Password Change	<u>Reset Password</u>
	AERS Provisioning Pa	ge <u>AERS Sales Pe</u>	ge

MACD Using the Provisioning Page

- 1. A Moves, Adds, Changes, Deletes (MACD) agent will receive the AERS order and spreadsheet within their MACD group mailbox.
- 2. The MACD agent is responsible for saving the spreadsheet into the pre-design folder on the network drive. The spreadsheet will be labeled as "[Pjob#] AERS Spreadsheet".
- 3. Log into the **AERS Tool** using the process described in *Logging into AERS*, and select the **AERS Provisioning Page**.
- 4. The first step is to select an Available Customer Names from the drop-down menu to ensure the same customer name is used. If for a new customer, cut-and-paste the customer name from the spreadsheet into New Customer Name.
- 5. Then cut-and-paste the Group ID number from the spreadsheet.
- 6. Type Sender's HRID from the information spreadsheet.
- 7. Using the Browse button locate the spreadsheet from network drive.
- 8. Click the Scrub button once the spreadsheet is identified.
- 9. Click on View Spreadsheet link to the spreadsheet just uploaded.
- 10. Click on View Report link to view a detailed report of the data retained from the spreadsheet.

Version 1.0.6 A Sep 200 Welcome Step 1. Fill out spreadsheet info	AT&T LOCAL PROVISIONING Start your net.working ERS (Alternate Enhanced Redirect Solutions) Step 2. Choose the file to upload	<u>Sales Page</u>
Required Upload Information	Local Machine	
Osuilable Container Manue	(Use this section to upload your spreadsheet to the server)	
Available Coloumet Names		Browse
New Customer Name	Step 3. Upload and scrub the file	Scrub
	View Spreadsheet. View Report	
Group ID		
Sender's HRID		
POST		

Note: If there are any errors received while attempting to import the spreadsheet, first check the spreadsheet for the appropriate format as described in the *Business Rules*. Then contact the AERS system administrator for assistance.

11. The MACD agent can click on View Spreadsheet or View Report to see details regarding the import.

Sales Using the AERS Sales Page

- 1. Log into the AERS Tool using the process described in Logging into AERS, and select the AERS Sales Page.
- 2. Select the Customer Name from the drop-down menu.
- 3. Select the appropriate **Group ID** for that customer.
- 4. There will be a maximum of two spreadsheets per customer saved within the AERS Web Tool.
- 5. Select the appropriate **Available Spreadsheets** from the drop-down menu.
- 6. Click on one of the options, **Spreadsheet**, **Report**, **Display Grid**, or **Compare Reports**, to review the data depending on your needs.

Version 1.0.6 AERS (A	AT&T LOCAL PROVISIONING Start your net.working Iternate Enhanced Redirect Solutions)	<u>Spreadsheet Template</u>	Provisioning Page
Welcome Step 1. Choose a customer Customer Name M Step 3. Choose a Spreadsheet Available Spreadsheets M -1000000001-01.xls Step 4. View the Spreadsheet and/or Report (if the spreadsheet has been scrubbed) Spreadsheet Report Diplay Grid * NT 4.0 users must right click the "Spreadsheet" link and choose "Save Target As"	Step 2. Choose a Group ID Group ID 1000000001 File Name: -100000001-01.xls Created on: 6/24/200 9:36:10 AM File Size: 404480 Last accessed: 8/21/200 11:12:44 AM Received: 6/24/200 9:36:00 AM Received: 6/24/200 9:36:00 AM Scrubbed: 6/24/200 9:36:00 AM Scrubbed by: 730 Compare Reports	NT 4.0 users must right click this link and choose "Save Target As"	

- 7. The **Spreadsheet** selection will allow you to view the Excel spreadsheet that MACD imported. You can right click to save the document onto your hard drive if needed.
- 8. The **Report** selection will allow you to review the following information:
 - ♦ AERS Report for (Customer Name)
 - ♦ Group Information (Total dialed TNs)
 - Error Information Specifics (These would need to be corrected)
 - Range Information
 - Redirected Number Information (From TN to TN, etc.)
 - ◆ Redirected NPA Information (From NPA to NPA, etc.)

AERS Report AERS Report for M , Group ID 1000000001 M New York, New York NYCY54HCE01 Spread Sheet - M -1000000001-01.xls Created on 6/24/200 9:36:13 AM By 730

Group Information

There were 5000 total Dialed TNs

Error Information

Group Info Tab There were no Group Info Errors

Control Number Tab

There were no errors

Customer Group Tab There were no Customer Group Errors

Range Information

There were a total of 1 ranges Range 1 Starts at 212 5000 and Ends at 21

5000 and Ends at 212 9999 For a total of 5000 lines

Redirected Number Information

Dialed TN redirected to different number

Note: The **AERS Tool** will advise you if there are no errors within the spreadsheet. If errors do exist, it is the original requestors responsibility to correct the errors within the spreadsheet and resubmit to the MACD team for importing.

9. The Display Grid selection will allow you to view the Dialed TN and the Options associated with the TN.

	AT	&т				ATO	TLOC								
2	Int	ranet				AIQ	Start ve	our net.w	orking	10					
ersion	1.0.6			4.57	200 (4)			1.7		a	1				
				AE	KS (AI	terna	ae Enh	ianced R	ledirect	Solution	ns)	Spreads	<u>neet Template</u>	Provisioning Page	
Wel	lcome											NT 4.0 u	sers must k this link and		
Step 1. Choose a customer				Step	2. Choo	se a Group	D			choose "Save Target					
Cust	tomer N	ame				Group	рD					As"			
М						100	0000001	•							
Step	3. CI	100se a S	Spreadsheet												
Avai	lable Sp	readsheets													
М		-1000	000001-01.×ls		•										
Step (if the Spree * NT	eadshe	ew the S eadshee eet <u>R</u> ers must i	preadsheet a t has been sc eport <u>D</u> right click the '	nd/or rubbed iplay ("Spread	Report l) <u>Jrid</u> sheet"	Com	pare Rep	orts							
muk a	and cho	iose Save	arget As"												
Line	Diale	dtn	BillingTN	Optic	m2	Optic	n3	Option4	OptionS	Option6	Option7	Option8	Option9		
2	212	5000		212	5000	212	5000		-				_		
4	212	5002		212	5002	212	5002				1				
5	212	5003		212	5003	212	5003								
6 7	212	5004		212	5004	212	5004								
8	212	5005		212	5005	212	5005								
9	212	5007		212	5007	212	5007								
10	212	5008		212	5008	212	5008				-				
11	212	5010		212	5010	212	5010	-	-						
13	212	5011		212	5011	212	5011						0		
14	212	5012		212	5012	212	5012		_			_			
10.	The (subm	Compa nitted.	a re Report For examp	s sele le, th	ection v is seled	vill all ction v	ow the will list:	user to \ "Optior	view the	differen ne # w	ces bet v as cha	veen mu nged f	ltiple spreads rom TN to	heets TN".	
		&T Intrane	t			AT&	T LOCA	AL PROV	ISIONIN orking	IG					
1,511,01	1.0.0			AE	RS (Al	terna	te Enh	anced R	edirect	Solution	15)	Spreadsh	ieet Template	Provisioning Page	
Welcome Step 1. Choose a customer					Step 2. Choose a Group ID						NT 4.0 users must right click this link and above "Sour Torret				
Cust	omer N	me				Groun	D					As"	Dave I alber		
M					¥	100	0000001	•							
Sten	3. CI	toose a S	Spreadsheet			There w	vere 270 cha	anges —							
			1			Compar	ison Repor	t for M	-100000	00001-01.xls	and M				
Available Spreadsheets					100000001-02:33 Option 2 Line 262 was changed from 212 5260 to 212 2383 Option 2 Line 644 was changed from 212 5642 to 201 6050 Option 2 Line 644 was changed from 212 5664 to 201 6050 Option 2 Line 644 was changed from 212 7606 to 732 2411 Option 2 Line 4913 was changed from 212 9911 to 201 9911 Option 3 Line 49 was changed from 212 5047 to 201 4848 Option 3 Line 64 was changed from 212 5054 to 201 5137 Option 3 Line 64 was changed from 210 6024 to 201 5137										
Step 4 View the Spreadsheet and/an Depart															
(if the spreadsheet has been scrubbed)										9911 4848 5137 5062					
<u>Spre</u> * NT link a	adshe 4.0 use ind cho	eet <u>R</u> ers must r ose "Save	eport <u>D</u> ight click the " Target As"	iplay (Spread	frid sheet"	Option 3 Line 64 was changed from 201 6230 to 212 5062 Option 3 Line 82 was changed from 201 0550 to 201 6267 Option 3 Line 83 was changed from 201 6090 to 201 6091 Option 3 Line 109 was changed from 212 5107 to 201 6203 Option 3 Line 125 was changed from 212 5123 to 201 6204 Option 3 Line 129 was changed from 212 5127 to 201 6200									

69

How to Break Into Medium–Security Installations

A Phile for the Aspiring Security Consultant

Date: Oct. 14, 1992 Revised: Sep. 15, 1993 Author: Terminal Technician 414 (TECH@902:414.00) Co-Author: Doctor Chaos 414 (CHAOS@902:414.00) Information From: C&M Security Systems staff (Thanx guys!) -(They're outta business now)-And of course personal experience.

Overview

For the purposes of this file, we'll consider any installations employing cipher or card locks and/or alarm systems to be "medium security." This covers nearly all department stores, some houses, warehouses, telephone company installations, and some government installations. Low-security installations are easy enough to break into, the most you'll need is a decent knowledge of lockpicking. High-security installations (military bases, prisons, arsenals, etc) are covered in another phile. This one will get you into most of the places you'll want to get into.

Part I: Exterior Perimeter Security

Many medium–security installations employ external perimeter security devices. These include the following:

- Fences
- Security Cameras
- Cipher Locks
- Card Readers
- Ordinary Everyday Locks --- For info, get a phile on lockpicking.

We'll cover these in that order. I'll try to include all the information you will need to identify and defeat each device. Well, on to the fun stuff!

Fences

The most common type of fence you will encounter is the cyclone or chainlink fence. There are three ways to deal with a simple cyclone fence:

- Cut through it: This method is fairly easy, but not recommended since it is obvious that someone has tampered with the fence. If you want to cut through it, you will need a wire cutter with fairly good leverage. If you try to use a cutter that is too small, you will take too long and will probably be caught. I recommend one of the following alternatives to this method of entry.
- Climb over it: This method is preferable if you can gain access to the fence in a dark or hidden area. Due to the fact that you are a very easy target to spot while climbing over, I recommend climbing only when you are sure you will not be seen.
- Crawl under it: This method is by far the preferred method if it is possible. Usually you can lift the fence up enough to squeeze under. The advantage to this method is that you will not be easily seen.

There are a few security devices that may be used in conjunction with fences. The most common is the vibration sensor. This consists of either a mercury switch or a steel ball on contacts. These can

be identified as a small box attached to the fence every 5 to 10 posts. Vibration sensors may be defeated either by being careful not to disturb the fence, or by searching for a tree or other tall object that you may jump from and land on the other side of the fence. Just make sure there's a way back out! Another device is the wire resistance sensor. This essentially turns the entire fence into a sensor. This device will detect strong vibrations, such as those created by climbing, as well as the increase in resistance caused by cutting. This type of sensor cannot be detected visually, but you can find them. Simply get a few medium sized rocks, throw them forcefully at the fence. If you're feeling confident, you can run up and shake the fence instead. After you've done one or the other, hide somewhere (not too close) and watch. If security personnel show up, you can assume some sort of sensor is in use.

Security Cameras

There are two main types of cameras: The constantly monitored variety, and the videotaped variety. The videotaped variety presents no major problems, just wear a disguise (ski masks work well) so you can't be identified. The constantly monitored type presents a problem. If you can't just walk around its field-of-view, and really want to get in, this method of defeating them works very well:

- Get a small VCR, preferably battery-operated, with video input and output jacks. The smaller and quieter the better.
- Attach the video input of the VCR to the output of the camera. Most cameras have a BNC connector on the back with a coaxial cable leading to the monitoring station. Strip the outer jacket from the coax for about two inches. Cut through some of the shield conductor (braided copper right inside the jacket). DO NOT CUT ALL OF IT. You should now have some stands suitable for connecting to. Now cut away some of the white stuff in the middle so you can get at the center conductor. Connect, with alligator clips or equivalent, the VCR video input to the center conductor and shield.
- Set the VCR on record, and let it record for as long as you plan to remain in the installation. Always best to add a few minutes for safety. When you're done, stop the VCR.
- When you have recorded for a while, disconnect the video input, and connect the video output of the VCR to the cable you stripped a while back. Press PLAY and remove the connector from the camera. It's best to leave the area briefly at this point, in case anyone investigates the slight picture disruption you will cause.

The security personnel will see your nice taped image of nothing going on, while you are carting out their equipment right in front of the camera. This technique works very well if properly executed, and very badly if you fuck it up. Advice: Get it right the first time -- You probably won't get another try if you fuck it up.

Cipher Locks

There are several types of these. The most popular ones you will find on non-military installations are made by Simplex. Two common types:

- The 1000 Series: A large silver box, with 5 buttons and a doorknob. You push the buttons in the correct sequence, then turn the knob. The best way to open these is to try likely combinations. If you don't know any likely combinations, you can try brute-force hacking of the combinations. The code can be one to five digits, using any combination of keys, and can also have two keys that must be pressed simultaneously. The number of possible combinations offered is around 3500. Maybe you'll get lucky.
- The 100 Series: A compact version of the 1000 Series. Has a small, elongated diamond shaped knob, with the buttons arranged in a circle above it. These are fairly easy to crack. The combinations arrangement is similar to that of the 1000 Series, only I do not think that multiple buttons can be pressed simultaneously. The number of possible combinations offered is about 1900.

Also, these days you will find digital cipher locks. They will usually have a keypad with digits 0 – 9. Most of these use a 4-digit code, but I have see some that use up to 12 digits. There are several ways to defeat these. One way is to just watch an authorized person enter the code, then go enter it yourself later. If this is not possible or practical, sometimes you can remove the unit from its mounting and find its output terminals. You can just short out the terminals, and off you go. If you want to get the code, you can apply a water-soluble ultraviolet ink to the keys. Once an authorized person enters the code 2 or 3 times, you can look at the keys with your ultraviolet light (WHAT? You don't have one??). You'll get the digits but not the sequence. Not a problem with cheap 4-digit ones, but getting 8, 10, or even 12 digits in the right order takes time, which you often will not have in abundance.

Most military installations have high-security cipher locks, with tens of thousands of combinations. These CAN be cracked, but it's not easy. That's another phile. These high-security locks are usually made by Medeco or Halcroft (I think that's the name...).

Card Readers

The card reader is one of the more secure devices available for exterior perimeter protection. There are two varieties, optical and magnetic. The optical type works by detecting a pattern of punched holes in a card, or reflective marks on the card's surface. Magnetic readers detect magnetized domains in a strip of magnetic tape similar to audio tape. Both of these CAN be fooled if you have patience. The magnetic ones can sometimes be defrauded by running an ATM or credit card through it, jiggling the card, moving it through very rapidly, or pulling it out half way through reading it. The optical ones can often be fooled by using an opaque card punched with holes. The best hole spacing is around 1/64 inch. Slide this contraption through the reader at varying speeds, and jiggle it, and maybe you'll get in. Another method that works is to remove the reader from its mounting, and find the output terminals that indicate a successful read. Just short those terminals, and you're in.

Part II: Interior Perimeter Security

There are several type of interior perimeter security devices. The ones you'll encounter in everyday illegal entry are:

- Glass Breakage Detectors
- Magnetic Reed Switches
- Infrared Beams
- Vibration Sensors
- Pressure Sensitive Mats
- Tripwires

Well, that list doesn't do you much good, so here's a discussion of each device:

Glass Breakage Detectors

These simple devices consist of a mercury switch in a box. All they do is detect major accelerations in any direction. The idea is, when you break the window, the sensor will fall down and set off the alarm. These can be identified as a small circular or rectangular device attached to the glass of a window. The best way to defeat them is to find another way of entry, or if you can find a big window, cut a hole in it with a glass cutter, avoiding the sensor of course, and crawl through the hole. You can also cut a hand–hole in door glass to reach the inside lock knob.
Magnetic Reed Switches

These sensors have two parts, a switch that mounts on the door frame, and a magnet that mounts on the door. The switch stays closed as long as the magnet is present, and when the magnet is taken away it opens the circuit and triggers the alarm. Magnetic reed switches can sometimes be identified as a pair of small rectangular boxes near a corner of the protected door. Some switches are built into the doorframe, and can only be seen when the door is open. It's best to look for them during a time when the door can be opend legally, then come back later armed with your knowledge of the position of the switches. They can be defeated by placing a strong magnet against the door, then opening it enough to reach in and place an alligator clip lead across the terminals of the switch, bypassing it.

Infrared Beams

This type of sensor sends a beam of invisible infrared light across a walkway. There are two types, retroreflective and through-beam. Retroreflective sensors have a reflector at the far end that sends the beam back to the transmitter, which is also a receiver. Through-beam sensors have a separate receiver unit on the other side of the protected area. These always operate along a straight line from the sender to the receiver. You can usually spot these during daylight hours, they are usually small cylindrical or rectangular objects on either side of a hallway, or a small room. One end may just be a reflector, a small, usually yellow device much like a automotive marker reflector. Once you know where the beams are, you can crawl under them, jump over them, or just avoid them. If you have special gear, you will be able to see the infrared beams and deal with them without finding the sensors first.

Vibration Sensors

These may be mounted on a wall, door, or window. They are rather sensitive, and will detect any fairly strong vibration within several feet of the sensor. These look much like a magnetic reed switch, only there is no magnet and most of them have a reset button. The reset button must be pressed to clear the sensor once it detects vibration. The only way to defeat these is to know where they are and avoid them. Pressing the reset button will do no good once the alarm has been set off. If you can get at one, say on an interior door, you can place an alligator clip lead across its terminals to disable it, do your thing, then press the reset button and remove the lead.

Pressure Sensitive Mats

These operate on the same theory as the mats that open the doors at supermarkets. When you step on one, it closes a circuit and triggers the alarm. Only one way to deal with these: Avoid them.

Tripwires

These are not used much since the advent of optical beam sensors, but you may encounter them. The tripwire is a fine wire, usually number 40 to 45 electrical wire, streched across a walkway and tightened. When the wire is broken, an electrical circuit is disrupted and the alarm is activated. To detect these, your best bet is to move slowly and watch downward for the wires or suspicious holes in walls where a wire may come through. These are very uncommon, not much to worry about, but they're covered for the sake of completeness.

Part III: Interior Area Security

Internal area security devices are some of the more devious devices to detect unwanted presence. These devices include:

- Passive Infrared Motion Detectors
- Other Motion Detectors
- Ammonia Sensors
- Charged Particle Sensors
- Pattern Recognition Systems
- Sound Sensors
- Guards

These devices all operate by detecting characteristics of human movement or presence in the protected area. A breakdown of each device.

Passive Infrared Motion Detectors

These employ a heat-sensitive cell. They detect large changes in overall radiated heat, infrared radiation, in their coverage area. They will detect a human or a large animal in their coverage area by detecting its body heat. They respond only to fairly rapid changes. They can be identified as small, usually white, devices of various shapes. If you trigger one you will usually see a small red light come on. These are best found during hours when your presence is not overly unwanted, so that you can become familiar with their location and coverage. These can be defeated by walking VERY slowly through their coverage area. Also, you can use an infrared beacon to fool them. This wonderful device produces IR radiation in the same wavelength as a normal human body, and will increase the intensity of the radiation over the course of 5 minutes or so, until the detector is "blinded" and you may move around freely. These beacons cost several hundred dollars, but hey, if it'll keep you out of jail, it's worth it...

Other Motion Detectors

These use ultrasound (high-frequency soundwaves) or microwaves to detect movement. These devices make use of the Doppler effect. They look much like passive IR sensors, and can usually be defeated in the same way.

Charged Particle Sensors

These devices give off negative ions, and detect the concentration of negative ions in the room air. Negative ions will attach to any object in the area, so entering the area will dramatically reduce the number of ions left in the air. These look similar to ammonia sensors but are usually mounted high on a wall, or on the ceiling. Again, these are not common in medium–security installations, since they cost about \$12,000 a pop. Charged particle sensors can be defeated by moving very slowly in their region of sensitivity, usually the entire room containing the sensor.

Pattern Recognition Sensors

These consist of a video camera attached to a computer. The computer is programmed to detect any objects that look remotely human in the camera's field–of–view. The camera has to see an object for about 1/16th of a second before it will recognize it. To defeat them, carry a large piece of cardboard or anything that will drastically distort the camera's view of your overall shape. Cardboard sheets with eyeholes work very well. These systems are also terribly expensive (on the order of \$15,000 for a four–camera system) so they are only used in such places as banks and sometimes in warehouses. I guess \$15,000 is cheaper than hiring guards for warehouses.

Sound Sensors

These are primitive devices that detect anything that's loud enough to be considered an illegal intruder. They vary greatly in reliability, and often do not work at all. These systems are usually impossible to spot, as they need only a tiny hole in a ceiling tile or wall for the microphone. If you suspect that sound sensors are in use, just be quiet. That's good advice in any situation, really.

Guards

The single most effective security system, provided they do their job. There are two kinds of guards, those that work for the company they are guarding, and those who work for security firms. The company employed type are generally more dangerous, since their job is on the line, where a guard working for a security firm would just get transferred to a new station. Most guards have fixed patterns in which they circulate about the premises, and if you study these patterns, you can find gaps where you can enter and work undetected. Guards are far more hazardous to the illegal enterist, since they can detain you on sight, where if an alarm goes off you have some time to run like hell. If you really want to break into a facility that has security guards patrolling, study their patterns and be VERY careful.

That about does it for security systems, now on to some helpful hints for getting into places. If you ever plan to use the information in this file, use common sense and a lot of caution. Keep in mind that 9 times out of 10, the security system you have just read about will not be used alone, but in combination. The only way you can be safe is to keep a sharp eye out for the distinguishing characteristics of ALL these systems. If you spot any systems at all, it's very likely there are more. Don't get over confident or ignorant, and you'll do fine. Unless you're a complete idiot, in which case, FUCK YOU.

Part IV: Key Points of Entry

The first step in getting into any place is finding a way in. All structures tend to have their weak points. Fences have gates, which are usually easier to crawl under than the rest of the fence. When trying to gain access to a building, try to choose a door that is in the shadows or away from an area where witnesses may be. As far as buildings go, the easiest way in is usually an overhead door. They can often be pried with a prybar enough to get your hands in and force the door. If an overhead door is not available, look for the weakest-looking hinged door. Usually you will find a door with a big enough gap at the latch for you to jimmy the latch or if needed cut off the bolt with a cutoff grinder. Be sure to check the hinge pins, some doors have them welded in, but many do not. They can be driven out with a hammer and screwdriver. Windows are another sometimes easy target. If they are not locked, you can just shred the screen, if there is one, and climb in. If they are locked, you can break a pane and remedy that situation easily enough. Breaking the glass in a window or door should be considered one of our last resorts, since that will prompt the security staff to increase the resistance to future entry. Some buildings will have electrically operated overhead doors. In that case, you can either use a scanning transmitter (you can buy one that scans the 13 – 49 MHz band for about \$50) if they are RF operated, or cut into the wires and short conductors until something happens. There are many possibilities, and how you go at getting in depends how badly you want to do so. Many large warehouses have storm sewer manholes in them, and a little trip through the sewers is never out of the question.

Part V: Tools and Supplies

One thing that will come in handy is a large collection of keys. I keep every key I ever find, and copy every one I have access to. Right now, I have around 2000 of them, all arranged by size, brand, and type of lock. With a collection that size, odds are good that one of them will get you in with a little wiggling. A set of lockpicks is also handy but not essential, since there are always other ways in. As for tools, your best bet is not to carry an arsenal of them with you, but to observe the site, find out what you will need, then get it. If you are caught on a site with a large supply of tools, there will be no doubt as to what you are doing. It's best to use cheap tools, so that if need be you can ditch them in a quick escape. Always wear gloves or coat your hands with a substance that will block your fingerprints. Rubber cement works well and still provides an excellent grip. I recommend acquiring the following tools and supplies if you do not have them already:

- Screwdrivers, regular and Phillips.
- An Allen wrench set.
- A small, lightweight hammer.
- Long (2-3 foot) and short (6" 1 foot) pry bars.
- A bag of alligator clip leads.
- A small jackknife.

All these supplies should run you maybe 20 bucks, depending where you buy them, and every one will come in handy sometime when you're out having phun.

Part VI: Tools and Supplies

One thing you'll find is that you never have a tool when you need one, or you don't have time to do something right. In that case, I offer a few suggestions on how to improvise simple tools on the spot to do what you need. Most cars come with a lugwrench, and really nothing works better for removing padlocks the quick way. Your car jack will come in handy some day when you need to open an overhead door. If you come across one of those cheap little locks with the zigzag keyhole (I believe warded lock is the proper term) you can make a pick by taking a paper clip and bending the end into a small U–shape, and twisting it in the keyhole. With practice you'll be able to open them faster than you could with the key. I recommend practicing this tactic at home, as well as carrying a premade pick with you. Carrying a tube of crazy glue with you is a good idea. If you are being chased, apply it to any doorknob your pursuer will have to touch within the next few seconds, and that will stop him in his tracks. There are many situations where you will be able to devise quick booby–traps to stop the security guy from catching you. Tip over a pile of junk on him, set something up for him to trip over, etc, etc...

Part VII: Miscellaneous – Thoughts and Insane Ramblings

This file has been provided because the few members of the Realm of Chaos enjoy doing these things, and enjoy helping others do them. If you plan to use this information, I must warn you, just having this information is NOT all you need. You need common sense, and you must be careful. Some people tend to get overconfident after a while, which is fine until they hit something they've never seen before and find that they've rushed in too fast. I know people who have been busted this way. One has been in jail for two years now. I've provided a lot of tips and techniques and explanations, but it's all worthless without some intelligence on your part. Another helpful hint: Work alone, or only with trusted friends. Too many people have been busted because a "friend" ratted on them. I know this from personal experience, and no I don't want to talk about it, thank you very much. If you want to practice the techniques I have presented in this file, it's best to do it in relatively insecure buildings. Once you get a feel for finding and disabling various types of security systems, you will be able to do it faster and with more accuracy, which is critical in this profession. If you can, find someone at a security equipment supplier who will let you look at the

various pieces of equipment and get an idea of what each device looks like. It will help you immensely to be able to tell the difference between a reed switch and a vibration detector in the dark. And finally, I really don't condone reckless vandalism, unless it's of a police department. There's really very little point in breaking into a telco building and going wild with a baseball bat. If you want to get yourself some equipment, go ahead. If you just want to snoop and learn, that's fine too, but don't wreck it for the rest of us. I think I've said enough now, I'm starting to sound like my mother. Have fun with your new skills and don't get busted!

(And if you DO, well, you didn't learn all your tricks from me!)

--==>> Credits <<==--

```
Terminal Technician 414 - Author, contributor
Doctor Chaos 414 - Editor, contributor
Cracker Jack 414 - Provider of lots of info on passive IR sensors
Digital Death 414 - Guinea pig and general purpose pest
```

Nortel DMS–100 Input/Output Device Maintenance Overview

Overview

To monitor, maintain, operate, and administer the Input/Output Device (IOD) subsystem, operating company personnel use the IOD level and the associated sublevels at the Maintenance and Administration Position (MAP) terminal.

The Input/Output Controller (IOC) and Input/Output Module (IOM) are the main components of the IOD subsystem. Both these components have a MAP sublevel that is accessed from the IOD level. This article provides an overview of IOC and IOM maintenance.

The following table shows where to find information about IOD MAP sublevels other than IOC and IOM:

Information on IOD MAP Sublevels				
IOD Sublevel	Location of Information	NTP Number		
Device Independent Recording Package (DIRP)	Magnetic Tape Reference Manual	297-1001-118		
	Feature Description Manual	297-8xxx-801		
	Hardware Description Manual	297-8xxx-805		
	Alarm and Performance Monitoring Procedures	297-8xxx-543		
	Trouble Locating and Clearing Procedures	297-8xxx-544		
	Recovery Procedures	297-8xxx-545		
	Routine Maintenance Procedures	297-8xxx-546		
	DMS-100 Family Commands Reference Manual	297-1001-822		
Distributed Processing Peripheral (DPP)	Distributed Processing Peripheral Recovery and Routine Maintenance Procedures	297-1001-537		
	Distributed Processing Peripheral Card Replacement Guide	297-1001-536		
	Alarm and Performance Monitoring Procedures	297-8xxx-543		

IOC Functional Description

The IOC user interface provides access to commands that allow operating company personnel to use IODs to enter machine controls, perform tests, and request information.

Maintenance and administrative IODs are in an Input/Output Equipment (IOE) frame or a Cabinetized Input/Output Equipment (CIOE) frame. The following sections describe IOE frame and the IODs.

Input/Output Equipment Frame

The IOE frame is a standard DMS–100 frame. The frame contains a Magnetic Tape Drive (MTD) and a Frame Supervisory Panel (FSP). The frame also contains an IOC, and a maximum of two Disk Drive Units (DDU). The FSP provides power, control, and alarm circuits for the frame hardware. *Figure 1* shows the locations of I/O equipment in an IOE frame.



Figure 1 – Input/Output Equipment Frame

Input/Output Controller

The IOC is an equipment shelf in the IOE frame (see *Figure 1*). The IOC provides an interface to the SuperNode or SuperNode SE Message Switch (MS) for a maximum of 36 IODs. The IOC also provides an interface to the Central Message Controller (CMC) in an NT40 switch. The IOC shelf is part of the maintenance and administration area. For enhanced reliability, each maintenance and administration area must have at least two IOC shelves. The DMS–100 switch can have a maximum of twelve IOCs. When you configure the switch to have a maximum of twelve IOCs, network capacity decreases as a result of hardware limits.

The device controller cards provide the interface between the IOC and the IODs. There are 26 slots in an IOC shelf. A maximum of nine of the slots can contain device controller cards. One of the slots contains the power converter for the shelf. Eleven of the slots contain filler faceplates. Two of the slots contain the IOC processor cards.

The following sections describe some of the more common maintenance and administration IODs.

Disk Drive Unit

A Disk Drive Unit (DDU) is a device used to store and retrieve DMS–100 information and data. The following are examples of DMS–100 information and data:

- Office Image Data
- Automatic Message Accounting (AMA) Data
- Journal File (JF) Data
- Operational Measurements (OM) Data

You can transfer data to or from a tape, or any other medium, to the DDU that stores the data. A DMS-100 office requires a minimum of two DDUs (DDU 0 & DDU 1).

SCSI Disk Drive Unit

The Small Computer Systems Interface (SCSI) DDU (NT1X55FA) is a disk drive mounted directly on an IOC card. The SCSI DDU (NT1X55FA) is also known as an IOC DDU. The SCSI DDU is based on the industry standard SCSI. The SCSI DDU provides a migration path to the Fault–Tolerant File System (FTFS) for all DDU applications.

The SCSI DDU occupies a single slot on the IOC shelf. The SCSI DDU replaces the disk drive controller card (NT1X55DA) and associated DDU in the DDU shelf.

Magnetic Tape Drive

A Magnetic Tape Drive (MTD) is a device that allows transfer of DMS–100 information to a permanent memory tape. The permanent memory tape can be external to the switch. You can transport the permanent memory tape. You can use the MTD to store and retrieve the same type of information as the DDU. The MTD allows transportation of data with the magnetic tape. The MTD also serves as the backup for the DDU. A DMS–100 office requires a minimum of one MTD.

Modem

A modem is an external device that allows computers to send and retrieve information over telephone lines.

Printer

A printer provides paper copies of reports that the system generates.

Visual Display Unit

Visual Display Unit (VDU) is a terminal that serves as the main entry point for maintenance and administration commands made by operating company personnel.

IOC Processor Cards

The IOC processor cards are the main component of the IOC. IOC processor cards are also called as common control cards because they are always provisioned. The IOC processor cards consist of the I/O message processor card (NT1X62) and the I/O terminator card (NT0X67). The following sections describe the IOC processor cards.

I/O Message Processor Card (NT1X62)

The I/O message processor card (NT1X62) contains a microprocessor that can connect serial message links to the message switch. The card can connect a parallel data bus to the separate device controller cards. The NT1X62 card controls the complete operation of the IOC.

I/O Terminator Card (NT0X67)

The I/O terminator card (NT0X67) contains terminating resistors for the parallel data bus of the IOC.

Power Converter Card (NT2X70)

The power converter card NT2X70xx supplies the voltage required by the cards in the IOC shelf. This card does not provide power redundancy. If the power converter card fails, power to the complete IOC shelf fails.

The NT2X70AF power converter is the current and preferred selection. Existing IOC shelves equipped with SCSI DDU may be equipped with power converter NT2X70AE cards, this is acceptable.

If an IOC shelf is equipped with at least one SCSI DDU (NT1X55FA), power converter cards NT2X70AA, NT2X70AB, NT2X70AC, or NT2X70AD must not be used to power the shelf.

IOC Device Controller Cards

The IOC contains Device Controller (DC) cards that control the activity of each IOD. The DC cards allow IODs to communicate with the rest of the DMS–100 switch. You can place device controller cards in any of the even–numbered IOC shelf slots from 4 to 20. An IOC shelf can contain a maximum of nine DC cards. Every DC card has four ports. The ports are numbered 0, 1, 2, and 3.

Device controller cards allow IODs to communicate with the DMS–100 switch. Device controller cards use the Electronic Industries Association (EIA) standard RS–232 interface or the Current Loop (CL) interface.

Figure 2 shows the locations of the DC cards in the IOC shelf.



Figure 2 – Device Controller Cards in the IOC Shelf

The following sections describe the DC cards that provide an interface with the main types of IODs.

Disk Drive Controller Card (NT1X55)

A disk drive controller card (NT1X55) provides an interface for one DDU. The DDU must be on port 0 at the MAP display. The NT1X55 card uses ports 2 and 3 to connect two control cables. Ports 0

and 1 are not equipped. A DMS–100 office requires two or more NT1X55s because the office requires two or more DDUs. The disk drive controller cards are in slot 4 of the shelves in IOE frame 0 and in IOE frame 1. The NT1X55 can pass message data to and from an I/O message processor card (NT1X62). See *Figure 3*.

Magnetic Tape Controller Card (NT1X68)

A magnetic tape controller card (NT1X68) provides an interface for one MTD. The MTD must be on port 0 at the MAP display. The NT1X68 card connects a read cable, a write cable, and a control cable. The card connects the cables with ports 1, 2, and 3 (in the order given). Port 0 is not equipped. Port 0 can pass message data to and from an I/O message processor card (NT1X62). See *Figure 3*.

Multi–Protocol Controller Card (NT1X89)

A Multi–Protocol Controller (MPC) card (NT1X89) allows data communications between a DMS–100 switch and an external computer. For example, a Central Office (CO) billing computer can have data communications with a DMS–100 switch. The system downloads the NT1X89 protocol software from the DMS–100 CPU. The NT1X89 protocol software supports software routines for Data Packet Network (DPN) communications. See *Figure 3*.

Terminal Controller Card (NT1X67)

A terminal controller card (NT1X67) provides an interface for a group of four devices. One of the devices can be a VDU. The NT1X67 card also provides an interface for any group of four printers (read–only or keyboard send–receive), or modems. The number of NT1X67 cards required depends on the number of console devices equipped in the DMS–100 switch. The NT1X67 card can pass message data to and from an I/O message processor card (NT1X62). See *Figure 3*.



Figure 3 – IODs Attached to the Device Controller Cards

IOM Functional Description

The IOM user interface provides access to commands that allow operating company personnel to use IODs to enter machine controls, perform tests, and request information.

Maintenance and administrative IODs are in the Integrated Services Module (ISM) shelf. The following sections describe the IOM and the associated IODs. The following sections also describe the ISM shelf, Integrated Services Module (ISME) frame, and Integrated Services Module (CISM) cabinet.

ISM Shelf

The ISM is a single shelf unit that replaces the current Trunk Module (TM) shelf or the Maintenance Trunk Module (MTM) shelf. The ISM shelf is on the Cabinetized Metallic ISM (CISM), the Frame ISM (FISM), or Cabinetized Metallic Test Access (CMTA). The CISM, FISM, and CMTA contain a maximum of four ISM shelves. The ISM shelf has the same functionality as current TM/MTM shelves. See *Hardware Description Manual*, NTP 297–8xxx–805 for a complete description of the ISM shelf.

ISME Frame

The ISME frame is a standard DMS–100 frame that supports a maximum of four ISM shelves. The Modular Supervisory Panel (MSP) provides power, and control for the frame hardware. *Figure 4* contains a schematic diagram of the IOM in an ISM positioned in an ISME frame.



Figure 4 – IOM Equipment in the ISM (ISME Frame)

CISM Cabinet

The CISM cabinet is a standard DMS–100 cabinet that supports a maximum of four ISM shelves and a cooling unit shelf. The Modular Supervisory Panel (MSP) provides power and control for the frame hardware. *Figure 5* shows a schematic diagram of the IOM in an ISM positioned in a CISM cabinet.



Figure 5 – IOM Equipment in the ISM (CISM Cabinet)

Input/Output Module

The Input/Output Module (IOM) is a direct replacement for the IOC shelf. The IOM provides all the functionality of the current IOC cards, with the exception of the NT6X91. The IOM with a Digital Audio Tape (DAT) and a Disk Drive Unit (DDU) replace the IOC and Magnetic Tape Drive (MTD). The IOM occupies three shelf slots. If a DAT is not required, the IOM controller cards provide 9–track MTD support.

The IOM supports all peripheral equipment that a completely provisioned IOC shelf supports.

The main IOM controller card (NTFX30) is in slots 3 or 4 of the Integrated Services Module (ISM). This card has all the communication ports and controller circuits for the storage media card. Together, the controller card and the storage media card provide all the communications and storage functions of a completely provisioned IOC shelf.

The storage media card (NTFX32AA) occupies slot 4 of the ISM shelf. The card has plug–in DAT (NTFX32CA) and DDU (NTFX32BA) units. The plug–in design gives maximum flexibility. The plug–in design does not require card replacement for upgrades and repairs. The NTFX31AA paddle board mounted on the rear of the backplane supplies power to the IOM smart connectors. The backplane supplies power to the NTFX32AA card directly.

The main controller card provides the interface between the IOM and the IODs. The card has twenty DS–30 communication ports. Sixteen ports are general–purpose input/output ports. The ports provide RS–232C, V.35, current loop, or PERTEC interfaces with a smart connector at the end of the cable for the protocol conversion. Communication with the message switch requires two DS–30 ports. The remaining ports are not used.

Smart connectors have a 6-pin Teledapt connector on the IOM side and a 25-pin connector on the user side. The PERTEC interface connects to the IOM through a 6-pin D-type connector on the IOM side. The interface also connects to the IOM through a 50-pin connector on the user side. The PERTEC conversion box is on the MTD in a vertical position. The cables from the box connect to the MTD or DPP.

The IOM controller card (NTFX34AA) has the option of setting the clock to internal or external. The option is only available when NTFX34AA is used as a MPC RS–232 port. For other synchronous configurations, the smart connector expects clock from the modem or external devices.

In external clocking modes with NTFX34AA, NTFX35AA, or NTFX35BA, the smart connector expects the external device to provide the receive clock and the transmit clock to be from the same source. The receive clock and the transmit lock should also be with the same frequency and locked in phase. The same frequency and locked in phase forces the user to set the same baud rate for both transmission and reception and disallows the use of modems that have limited clocking features with IOM. This is not in alignment with the IOC operation, and the solution is to replace the modem with another modem.

Device	Make/Model	СРС	Connector
Printers	DEC LA75/424 (MD) DEC LA30 (Narrow Carriage) DEC LA400 (Wide Carriage)	- A0660002 A0660949	6-pin MMJ 6-pin MMJ 6-pin MMJ
Terminals/VDUs	DEC VT320/340/420 (MD) DEC VT520 DEC VT525	- A0661478 A0385880	DB25M, 6-pin MMJ DB25F, DB25M, 6-pin MMJ DB25F, DB25M, 6-pin MMJ
Modems/Data Sets			
GDC Modems	GDC, DS 6/R 1 Modem Shelf	A0602127	DB25F
	DC 202S/T	A0328522	DB25F
	DC 9600 RPA	A0378922	DB25F
	DC 596	A0351816	DB25F
	DC 596X.25	A0378945	DB25F
	DT VFAST (RS-232) 28.8K	A0620530	DB25F
	DC 500G/UXR	A0632487	DB25F
	DC 500F/AXR	A0614226	DB25F, V.35
	DT 500A	A0386041	DB25F
	NMS 510/IFP	A0605210	DB25F
	NMS 510	A0640834	DB25F
	DT VFAST 28.8K V.35	A0620540	DB25F

The following table lists supported I/O devices for IOM and the type of its connectors:

UDS/Motorola			
Modems	UDS RM16M Modem Shelf	A0344310	DB25F
	DC 202S/T	A0336496	DB25F
	2440	A0360824	DB25F
	DDS/MRS ADPT	A0609600	DB25F
	DDS/MR1 RS-530	A0600483	DB25F
	V.3229	A0600471	DB25F
	DU 170 RS-232	A0633604	DB25F
	DU 170 RS-530	A0636941	DB25F
Rixon Case/Osicom	RM4200 Modem Shelf	A035525	DB25F
Modems	DCM4202	A0355257	DB25F
	DCM4212	A0355260	DB25F
	DCM4229	A0355256	DB25F
	DCM4222	A0351638	DB25F
	DCM4232	A0352027	DB25F
	DCM4296	A0351641	DB25F
	DCM4256	A0385841	DB25F

-End-

The following sections describe the maintenance and administration IODs that correspond to the IOM.

IOM Subsystem Components

The IOM controller card (NTFX30AA) and the associated paddle board (NTFX31AA) are the main components of the IOM. The following sections describe the IOM cards.

IOM Controller Card (NTFX30)

The IOM controller card (NTFX30) contains hardware and firmware to support 16 general–purpose ports. The ports include the RS–232C, V.35, current loop and PERTEC. The hardware and firmware also support two DS–30 links to the message switch and two optional external SCSI devices on the storage media card. The NTFX30 controls the emtire operation of the IOM.

IOM Paddle Board (NTFX31)

The IOM paddle board (NTFX31) contains the power feed circuits. The paddle board contains a maximum of 16 smart connectors and circuits. The paddle board implements a local loopback for diagnostic purposes. The paddle board is at the rear of the backplane at the slot 3 position. The paddle board has 20 connectors. Sixteen connectors supply power and the signal to the smart connector at the end of the cable. The four connectors that remain do not have power. Two of the connectors have connections to the message switch and the last two are not used.

IOM Storage Media Card (NTFX32)

The IOM storage media card (NTFX32) is an optional unit for the IOM. The media card holds the 3.5–inch DDU (NTFX32BA) and/or DAT (NTFX32CA) units. With these units installed, the media card is functionally equivalent to the IOC DDU and/or 9–track MTD. You can use the media card in all applications that require a DDU and/or 9–track MTD.

Disk Drive Unit

The IOM 3.5–inch DDU (NTFX32BA) has a capacity of 2–GByte. The DDU performs the same function as the current IOC SCSI DDU. The disk drive unit is on the IOM storage media card. The

DDU is based on the industry standard SCSI.

Digital Audio Tape Unit

The DAT unit (NTFX32CA) has a capacity of 1.3–GBytes (not compressed). The DAT unit performs the same function as the IOC MTD. The DAT unit is on the IOM storage media card.

Bulkhead Splitter Unit (NTFX39)

The bulkhead splitter unit (NTFX39) is a one-to-nine cable splitter unit for the cabinetized ISM.

Fault Conditions (IOC and IOM)

Fault conditions in the IOC or IOM are caused by product design, product defects, or product failures during operation.

The IOM uses the same alarm indications as the IOC. The alarm clearing procedures for the IOM are different than the procedures for the IOC. The following sections explain the IOC and IOM level fault conditions.

Babbling Device

The babbling device fault occurs when a device sends an excessive quantity of I/O interrupt messages to the message switch. This condition is referred to as *babbling*. The message switch detects the babbling device when the quantity of I/O interrupt messages exceeds the threshold. When babbling starts, the babbling remains until maintenance actions correct it. The babbling device thresholds are set at low, medium, and critical. Removal of the IOD from service occurs for medium or critical levels.

Circuit Error

A Circuit Error (CKEr) fault occurs when one or more I/O or IOM devices disconnects at the IOC end of the link to the IOC or IOM.

Circuit Out-of-Service

For IOC, the Circuit Out–of–Service (CkOS) fault occurs when there is a problem with the terminal controller card (NT1X67). When the CkOS fault condition occurs, there is no service to devices connected to the NT1X67 card .

For IOM, the CkOS fault occurs when a controller port is out–of–service. When a controller port is out–of–service, there is no service to devices connected to the NT1X67 card.

Disk Drive Unit Out-of-Service

For IOC, the Disk Drive Unit Out–of–Service (DDUOS) fault occurs when there is a problem in the disk drive controller card (NT1X55).

For IOM, the DDUOS fault occurs when one or more of the DDUs are out-of-service.

If the DDUOS fault occurs, you cannot record or download files to or from tape, or the DDU.

Input/Output Controller Out-of-Service

For IOC, a problem in one of the IOC processor cards causes the Input/Output Controller Out–of–Service (IOCOS) fault condition. The IOC processor cards are the I/O message processor card (NT1X62) or I/O terminator card (NT0X67).

For IOM, a problem in the IOM controller card (NTFX30) causes the IOCOS fault condition.

When the IOCOS fault condition occurs, all devices associated with the out–of–service IOC lose communication with the DMS–100 switch.

Multi-Protocol Controller Out-of-Service

For IOC, the Multi–Protocol Controller Out–of–Service (MPCOS) fault occurs when there is a problem in one or more multi–protocol controller cards (NT1X89). Remote terminals lose access to the DMS–100 switch for any affected cards.

For IOM, the MPCOS fault occurs when there is a problem with one or more multi–protocol ports. Remote terminals lose access to the DMS–100 switch for any affected ports.

Magnetic Tape Drive Out-of-Service

For IOC, the Magnetic Tape Drive Out–of–Service (MTDOS) fault condition occurs when there is a problem in the magnetic controller card (NT9X68). If the Device Independent Recording Package (DIRP) utility uses the MTD to record billing data, loss of billing data occurs. If the DIRP utility does not use the MTD, you cannot download or record files to or from tape.

For IOM, the MTDOS or Digital Audio Tape Out–of–Service (DATOS) fault condition occurs when there is a problem in one or more magnetic tape drives or digital audio tapes. If the DIRP utility uses the MTD or DAT to record billing data, loss of billing data occurs. If the DIRP utility does not use MTD or DAT, you cannot download or record files to or from tape.

Automatic Maintenance

The system performs self-diagnostics. The system isolates and tests an IOD component that has faults. The system attempts to return the component that has faults to service.

Manual Maintenance

When the system cannot clear an alarm, perform manual actions to clear the alarm. Perform manual maintenance on a periodic schedule according to local operating company policy.

Motorola Bag Phone Handset Control

Overview

An experimental control circuit to simulate the handset key presses on an old Motorola "bag"–style cellular phone. Refer to *GBPPR 'Zine*, Issue #4 for an application on using two old cellular phones to jam tape recorders.

A standard Microchip PIC16F84 is used to control two 4066 quad bilateral switches, which in turn, simulate pressing the keys on the keypad. Wires are run from the 4066s to each *row* and *column* on the handset's keypad. When a connection is made from the row to the column, the phone registers a key press. The source code for the PIC16F84 is written in PICBasic, so it's very easy to understand. The code, as written, takes about ten seconds to execute.

For this design, you'll only need to control the keys: 1, 2, 3, 7, 8, 0, and #

The key sequence will be like this:

[#] - Enter the test mode's servicing level.
 [1] [1] [0] [0] [1] [#] - Enter channel '0001' for a transmit frequency of 825.03 MHz.
 [2] [8] [#] - Enable the high tone of 1,150 Hz.
 [3] [0] [#] - Enable the low tone of 770 Hz.
 [1] [2] [0] [#] - Set the maximum transmit RF power of 3 Watts.
 [2] [7] [#] - Continuously transmit control channel data.

This makes a nice "warbly" jamming noise signal, useful for jamming tape recorders.

Keypad Connections

Pictures



Handset overview. An example keypad circuit board is shown on the left.



Taking the handset apart. There are usually three screws, two T6 Torx and a T8 Torx.



Close up picture of the microphone (right), speaker, and handset cable connector.

The pinout and wire color for the RJ-45 connector is as follows:

- 1. BLUE Handset Logic Ground
- 2. RED +9.5 VDC
- 3. PURPLE T-DATA, 3-Wire Databus "True"
- 4. **ORANGE** C–DATA, 3–Wire Databus "Complimentary"
- 5. YELLOW R-DATA, 3-Wire Databus "Return"

- 6. BROWN Handset Audio Ground
 7. GREEN No Connection
 8. WHITE Receive Audio to Handset



Internal view. Clear out all the nonsense.



Close up of the keypad and its connections. We'll only be interested in the twelve top pads. Note the three columns (going up and down) and the four rows (going across). We'll number the columns C1, C2, and C3 and the rows R1, R2, R3, and R4.



To remove the solder mask on the circuit board (to make testing with a continuity meter easier), use a Dremel tool with a wire brush attachment.



Close up picture of the keypads with the solder mask removed.



Control circuit board. PIC16F84 is on the top left, the two 4066s are on the bottom.



You may want to remove the little conductive pads behind the rubber keys. This will help prevent any accidental key pressing during operation.



Installation of the three row wires and the three column wires. You'll have to pin them out to double check them. Yes, it's a pain. Have fun!



Installation is complete. This was an experimental version, so it's a little messy.



Power the circuit from the +9.5 VDC line on the handset connection.

Schematic



PICBasic Source Code

```
' Motorola Bag Phone Handset Control
' Phone must be hardwired into test mode (ground pin 21 on the DB-25)
' PICBasic and PIC16F84-04I/P (4 MHz clock)
' See GBPPR 'Zine, Issue #4 - Use Old Cellular Phones to Jam Tape Recorders
       ' Bring all pins low
Low 0 ' 1
Low 1 ' 2
Low 2 ' 3
Low 3 ' 7
Low 4 ' 8
Low 5 ' 0
Low 6 ' #
Pause 4000
           ' Wait 4 seconds for things to settle
            ' [#] Enter Servicing Level
Gosub Pound
Pause 200
Gosub One
           ' [110001#] Set TX Frequency (825.03 MHz)
Gosub One
Gosub Zero
Gosub Zero
Gosub Zero
Gosub One
Gosub Pound
Gosub Two
            ' [28#] High Tone Enable (1150 Hz)
Gosub Eight
Gosub Pound
Gosub Three ' [30#] Low Tone Enable (770 Hz)
Gosub Zero
Gosub Pound
Gosub One
          ' [120#] Maximum TX Power (3 Watts)
Gosub Two
Gosub Zero
Gosub Pound
Gosub Two
             ' [27#] TX Continuous Control Channel Data
Gosub Seven
Gosub Pound
End
Pound:
      High 6
       Pause 200
       Low 6
       Pause 200
       Return
One:
       High 0
       Pause 200
       Low 0
       Pause 200
       Return
```

Two: High 1 Pause 200 Low 1 Pause 200 Return Three: High 2 Pause 200 Low 2 Pause 200 Return Seven: High 3 Pause 200 Low 3 Pause 200 Return Eight: High 4 Pause 200 Low 4 Pause 200 Return Zero: High 5 Pause 200 Low 5 Pause 200 Return

PIC16F84 Hex Code

```
:100000028288F018E00FF308E07031C8F07031CEA
:10001000232803308D00DF300F2003288D01E83EB8
:100020008C008D09FC30031C18288C070318152838
:100030008C0764008D0F15280C181E288C1C222894
:100040000002228080083130313831264000800B1
:1000500006108316061083128610831686108312EC
:1000600006118316061183128611831686118312D8
:1000700006128316061283128612831686128312C4
:1000800006138316061383120F308F00A030022050
:100090006120C83001206E206E20AF20AF20AF203D
:1000A0006E2061207B20A22061208820AF2061206B
:1000B0006E207B20AF2061207B2095206120630093
:1000C0005F28061783160613C83083120120061313
:1000D00083160613C8308312012008000614831605
:1000E0000610C83083120120061083160610C8308F
:1000F000831201200800861483168610C8308312EC
:100100000120861083168610C83083120120080053
:10011000061583160611C8308312012006118316B6
:100120000611C83083120120080086158316861137
:10013000C83083120120861183168611C8308312BD
:1001400001200800061683160612C830831201200B
:10015000061283160612C830831201200800861684
:1001600083168612C83083120120861283168612E7
:08017000C830831201200800D1
:02400E00F53F7C
:0000001FF
```



	U.S. Department of Justio United States Marshals Service
WAN BY U.S. N	NTED
NOTICE TO ARRESTING AGENCY: Before arrest, validat United States Manihals Service NCIC entry number: (NBC/	te warrant through National Crizes Information Center (NCIC).
NAME:	VIN DAVID
AKS (S):	IN DAVID
DESCRIPTION: Sex:	ALIFORNIA D/18/70 EPM19PM09
ADDRESS AND LOCALE: KNOWN TO RESIDE IN TH LAS VEGAS, NEVADA	HE SAN FERNANDO VALLEY AREA OF CALIFORNIA AND
WANTED FOR: VIOLATION OF SUPERVISED REL ORIGINAL CHARGES: POSSESSION UNAUTHORIZI Warnant hunde: CENTRAL DISTRICT OF CALIF Warnant Number: 9312-1112-0154-C DATE WARRANT ISSUED: NOVEMBER 10, 1992	EASE ED ACCESS DEVICE; COMPUTER FRAUD FORMIA
MISCELLANEOUS INFORMATION: SUBJECT SUFFER VEHICLE/TAC INFORMATION:	ES FROM A WEIGHT PROBLEM AND MAY HAVE EXPERIENCED
Research and the order that the second	She West Office (The see are the see a
If no answer, call United States Marshale Service Communic Telephone (800)336-0102: (24 hour telephone contact	cations Center in McLean Virginia. :i) NLETS access code is VAUSMOOOO.
PRIOR EDITIONS A	THE OBSOLETE AND NOT TO BE USED (Rev. 3/2/82

November 1992

End of Issue #22



Any Questions?

Editorial and Rants

We must remember to be tolerant of other people's cultures.

Pakistani Killed Daughters to Save 'Honor'

December 28, 2005 - From: news.yahoo.com

By Khalid Tanveer, Associated Press Writer

MULTAN, Pakistan – Nazir Ahmed appears calm and unrepentant as he recounts how he slit the throats of his three young daughters and their 25–year old stepsister to salvage his family's "honor" – a crime that shocked Pakistan.

The 40-year old laborer, speaking to The Associated Press in police detention as he was being shifted to prison, confessed to just one regret — that he didn't murder the stepsister's alleged lover too.

Hundreds of girls and women are murdered by male relatives each year in this conservative Islamic nation, and rights groups said Wednesday such "honor killings" will only stop when authorities get serious about punishing perpetrators.

The Independent Human Rights Commission of Pakistan said that in more than half of such cases that make it to court, most end with cash settlements paid by relatives to the victims' families, although under a law passed last year, the minimum penalty is 10 years, the maximum death by hanging.

Ahmed's killing spree --- witnessed by his wife Rehmat Bibi as she cradled their 3 month-old baby son --- happened Friday night at their home in the cotton-growing village of Gago Mandi in eastern Punjabprovince.

It is the latest of more than 260 such honor killings documented by the rights commission, mostly from media reports, during the first 11 months of 2005.

Bibi recounted how she was woken by a shriek as Ahmed put his hand to the mouth of his stepdaughter Muqadas and cut her throat with a machete. Bibi looked helplessly on from the corner of the room as he then killed the three girls –– Bano, 8, Sumaira, 7, and Humaira, 4 –– pausing between the slayings to brandish the bloodstained knife at his wife, warning her not to intervene or raise alarm.

"I was shivering with fear. I did not know how to save my daughters," Bibi, sobbing, told AP by phone from the village. "I begged my husband to spare my daughters but he said, 'If you make a noise, I will kill you."

"The whole night the bodies of my daughters lay in front of me," she said.

The next morning, Ahmed was arrested.

Speaking to AP in the back of police pickup truck late Tuesday as he was shifted to a prison in the city of Multan, Ahmed showed no contrition. Appearing disheveled but composed, he said he killed Muqadas because she had committed adultery, and his daughters because he didn't want them to do the same when they grew up.

He said he bought a butcher's knife and a machete after midday prayers on Friday and hid them in the house where he carried out the killings.

"I thought the younger girls would do what their eldest sister had done, so they should be eliminated," he said, his hands cuffed, his face unshaven. "We are poor people and we have nothing else to protect but our honor."

Despite Ahmed's contention that Muqadas had committed adultery — a claim made by her husband — the rights commission reported that according to local people, Muqadas had fled her husband because he had abused her and forced her to work in a brick–making factory.

Police have said they do not know the identity or whereabouts of Muqadas' alleged lover.

Muqadas was Bibi's daughter by her first marriage to Ahmed's brother, who died 14 years ago. Ahmed married his brother's widow, as is customary under Islamic tradition.

"Women are treated as property and those committing crimes against them do not get punished," said the rights commission's director, Kamla Hyat. "The steps taken by our government have made no real difference."

Activists accuse President Gen. Pervez Musharraf, a self-styled moderate Muslim, of reluctance to reform outdated Islamized laws that make it difficult to secure convictions in rape, acid attacks and other cases of violence against women. They say police are often reluctant to prosecute, regarding such crimes as family disputes.

Statistics on honor killings are confused and imprecise, but figures from the rights commission's
Web site and its officials show a marked reduction in cases this year: 267 in the first 11 months of 2005, compared with 579 during all of 2004. The Ministry of Women's Development said it had no reliable figures.

Ijaz Elahi, the ministry's joint secretary, said the violence was decreasing and that increasing numbers of victims were reporting incidents to police or the media. Laws, including one passed last year to beef up penalties for honor killings, had been toughened, she said.

Police in Multan said they would complete their investigation into Ahmed's case in the next two weeks and that he faces the death sentence if he is convicted for the killings and terrorizing his neighborhood.

Ahmed, who did not resist arrest, was unrepentant.

"I told the police that I am an honorable father and I slaughtered my dishonored daughter and the three other girls," he said. "I wish that I get a chance to eliminate the boy she ran away with and set his home on fire."

Do as I say, not as I do.

Mexico Admits Poor Treatment of Migrants

December 21, 2005 - From: abcnews.go.com

By Mark Stevenson, Associated Press Writer

MEXICO CITY Dec 21, 2005 -- Mexico's federal Human Rights Commission acknowledged on Wednesday that the country uses some of the same methods in dealing with illegal migrants that it has criticized the United States for employing.

The admission comes as Mexican Foreign Relations Secretary Luis Ernesto Derbez called on Latin American countries to unite against a U.S. House of Representatives bill to toughen border enforcement.

The bill, which passed on Friday with a 239–182 vote, would make illegal entry a felony, and enlist military and local police to help stop illegal entrants.

But officials of Mexico's federal Human Rights Commission acknowledged that Mexico already employs both tactics in its own territory.

"As a matter of fact, (Mexico's) population law does include prison terms for illegally entering the country ... and this is something that has been the subject of constant complaints," said Mauricio Farah, a national inspector for the rights commission.

Jose Luis Soberanes, president of the rights commission, said that Mexico also uses many government agencies, such as the police and the military, to detain undocumented migrants, even though Mexican law technically doesn't allow that.

"One of the saddest national failings on immigration issues," Soberanes told a news conference, "is the contradiction in demanding that the North (the United States) respect migrants' rights, which we are not capable of guaranteeing in the South," along Mexico's border with Guatemala.

But Soberanes slammed another provision of the U.S. immigration bill that would build 700 miles of additional fences or walls along the U.S.–Mexico border, calling it "absurd."

The commission also acknowledged that Mexico mistreats many migrants mostly Central Americans who cross Mexico in a bid to reach the United States and called for improvement on that front.

The human rights commission also presented a report on Wednesday that found overcrowding and bad conditions at about three–quarters of Mexico's 51 immigration detention centers and 68 other holding facilities.

The biggest problem with Socialists is that the only thing they care about, is money. France and Germany also pulled in the most profit from selling just about anything to Saddam Hussein. Hmmm.... I'm sure Manny Golddigger will mention this at HOPE 2006!

EU Arms Flow to China Despite Ban

December 13, 2005 - From: upi.com

By Gareth Harding, UPI Chief European Correspondent

BRUSSELS, Dec. 13 (UPI) -- Despite the European Union's arms embargo against China, EU weapons manufacturers bagged \$405 million worth of licenses to sell military goods to the communist state and exported a further \$86 million of hardware in 2004, official figures obtained by United Press International show.

The EU banned arms sales to China in 1990 in response to the Tiananmen Square massacre a year earlier. But this did not stop arms manufacturers from eight of the bloc's 25 members exporting military equipment to the world's most populous country last year.

"The figures seem to make a bit of a mockery of the European Union's claim that the arms embargo is still in place," said Roy Isbister of the London–based advocacy group Saferworld.

"The spirit of the 1990 statement is that military goods should not be exported to China, but member states are interpreting this in very different ways."

France, which has lobbied aggressively for the arms embargo to be lifted, would be by far the biggest beneficiary of such a move.

According to Council of Ministers figures, \$81 million of the \$86 million worth of military goods exported from the European Union were sold by French companies. It also ranks first in terms of the value of export licenses issued by governments, with orders totaling \$202 million given the green light last year.

Britain, which is lukewarm about lifting the embargo, came in at second place, with over \$175 million of licenses granted to its companies.

Governments have been able to bypass the embargo because the 1990 ruling is non-binding and only applies to weapons systems, not components or so-called "dual use goods" that have both military and civilian uses.

"The European Union does not have an arms embargo to speak of at this moment," says Tomas Valasek, Director of the Brussels office of the World Security Institute think-tank. "Each EU member state is left to its own devices about how to interpret the embargo -- which can lead to some strange situations. Some of the biggest proponents of lifting the ban, for example Germany, sell nothing to China; whereas some of the biggest opponents -- the British, for example -- sell more than anyone except the French."

France and Germany last year pushed for the arms embargo against Beijing to be lifted, stating that China had moved on from Tiananmen Square days. Most European states appeared to back the move, but after fierce resistance from the United States, the issue was quietly shelved.

"It is quite clear that the main reason the embargo is still in place is because of the United States," says Isbister.

The annual report from the Council of Ministers, which represents EU governments in Brussels, also reveals that European arms makers were granted licenses to sell \$4.3 million of military goods to Uzbekistan in 2004.

Last month the Union placed an arms embargo on the Central Asian republic in protest of the massacre of demonstrators in Andijan.

EU governments also granted arms manufacturers licenses to sell almost \$143 million worth of military goods to Venezuela and \$48 million to Iran -- two countries Washington is less than keen to see armed to the teeth with the latest military hardware.

Eurosavages need to shut the fuck up and fix their own problems. I wonder how much carbon dioxide Auschwitz or burning cars put out?

EU States That Berated Bush on Kyoto Fail to Hit Emissions Targets

December 27, 2005 - From: news.scotsman.com

By Alison Hardie, Senior News Writer

MANY of the European nations responsible for coercing the United States to remain committed to combating climate change are named and shamed today as major polluters of the environment.

A remarkable report has discovered Britain stands almost alone among 15 EU nations in making strides towards honouring Kyoto commitments to cut greenhouse gases.

The London–based think–tank, the Institute for Public Policy Research (IPPR), has found that ten of the 15 European Union signatories to the Kyoto Protocol will miss their targets by 2010 without urgent action.

The worst offenders are Spain, Portugal, Ireland and Italy, each up to 20 per cent off target. Only Britain, Sweden and France are remotely on target.

The poorly performing nations are among the many who have criticised the US and President George Bush – who early in his presidency declared Kyoto "dead" – for refusing to sign up to the agreement because of fears it would limit economic growth.

However, earlier this month – after fierce negotiations at a United Nations conference in Montreal, Canada – the US did agree to a "non–binding dialogue to respond to climate change", aimed at setting new mandatory limits on greenhouse gas emissions after 2012, when the existing pact known as the Kyoto Protocol expires.

The research carried out by the IPPR, the Left–leaning think–tank, finds that Britain has the best record on reducing greenhouse gas emissions. It projects that by 2010, with green policies still to be introduced, the UK will have reduced emissions by 20 per cent of the level recorded in 1990. Sweden will be just 1 per cent away from achieving its target of an increase on 1990 levels of just 4 per cent.

However, Spain will miss – by 13 per cent – its target of limiting emission levels to 15 per cent more than were recorded in 1990. Ireland will fail to hit its target of emission levels running at a rate of 13 per cent higher than the 1990 level by 20.4 per cent.

Duncan McLaren, the chief executive of Friends of the Earth Scotland, said last night he was surprised the IPPR had found the UK's projected performance would be so good, and he questioned its methodology.

However, he added: "We are not surprised to see the EU falling behind its Kyoto targets, and this is because nations are increasing the pursuit of economic growth rather than sustainable development."

Mr McLaren said the report did illustrate how quickly environmental policies could impact in a positive way.

The IPPR report said that although Austria on current performance was 21 per cent off its target, by 2010 after additional green policies had been adopted, it would miss its target by just under 4 per cent.

Austria's target is for emissions by 2010 to be 13 per cent less than was recorded in 1990.

Tony Grayling, IPPR's associate director, said: "We have very little time left to start reducing global greenhouse gas emissions before irreparable damage is done. It is vital that EU countries keep their promises to cut pollution."

At Kyoto in 1997, industrialised nations agreed to reduce their greenhouse gas emissions by 5.2 per cent relative to the 1990 levels by the period 2008–2012. The targets varied: a 20 per cent cut was pledged by Germany; 12.5 per cent by the UK; 7 per cent by the US; while some countries, such as Australia, negotiated large increases.

Wait... About 30 seconds ago, didn't we read about Eurosavages illegally arming a Communist dictatorship? LOL! Remember, Adolf Hitler would revoke your citizenship if you didn't agree with him.

Europeans Outraged at Schwarzenegger

December 13, 2005 - From: www.breitbart.com

By Vanessa Gera, Associated Press Writer

VIENNA, Austria – The execution of convicted killer Stanley Tookie Williams sparked outrage Tuesday throughout Europe, which has a deep aversion to capital punishment sustained by the painful memory of state–organized murder during the Nazi era. The disappointment was particularly strong in Austria, native country of Gov. Arnold Schwarzenegger, where many had hoped the former bodybuilder and filmstar would spare the 51–year–old Williams.

Leaders of Austria's opposition Green Party even called for Schwarzenegger to be stripped of his Austrian citizenship – a demand rejected by Chancellor Wolfgang Schuessel as "absurd" despite his government's opposition to the death penalty.

Capital punishment is illegal throughout the European Union, and the issue was amplified in Williams' case due to the remorse supporters believe the Crips gang co-founder showed by writing children's books about the dangers of gangs and violence.

Schwarzenegger rejected that argument and allowed the execution to go ahead Tuesday, saying "without an apology and atonement for these senseless and brutal killings, there can be no redemption."

Williams was convicted in connection with four killings during a pair of armed robberies in 1979. But he never wavered from his claim of innocence and refused to confess to crimes he did not commit, even if doing so would save his life.

Six decades after World War II, opposition to the death penalty remains deeply entrenched in Germany and Austria, a stance resulting from remorse for the evils committed by these countries under Adolf Hitler and an attempt to prevent future state–sponsored killing.

Volker Beck, a leading member of the opposition Greens party in Germany, expressed disappointment at the execution. "Schwarzenegger's decision is a cowardly decision," he told the Netzeitung online newspaper.

In Graz, Schwarzenegger's hometown, local Greens said they would file a petition to remove the California governor's name from the city's Arnold Schwarzenegger Stadium. A Christian political group suggested it be renamed for Williams.

"Mr. Williams had converted and, unlike Mr. Schwarzenegger, opposed every form of violence," said Richard Schadauer, chairman of the Association of Christianity and Social Democracy.

At the Vatican, Pope Benedict XVI's top official for justice matters denounced the execution.

"We know the death penalty doesn't resolve anything," said Cardinal Renato Martino. "Even a criminal is worthy of respect because he is a human being. The death penalty is a negation of human dignity."

Most of the outcry in Europe came from opposition political parties, city leaders, human rights groups and churches, with national leaders remaining silent.

"Schwarzenegger has a lot of muscles, but apparently not much heart," French Socialist Party spokesman Julien Dray told RTL radio.

In Italy, Franco Danieli, vice president of the Senate's Foreign Affairs Committee, criticized executions as an act of "dehumanization."

"The execution of Tookie Williams is even more intolerable exactly because he had managed to transform the negative into the positive, violence into nonviolence," Danieli said.

Amnesty International also condemned the execution.

"Tookie Williams' violent past was well known, but he had become a textbook version of rehabilitation and his execution was a travesty of justice," said Kate Allen, the group's director in Britain.

Rome's Colosseum, once the arena for deadly gladiator combat and executions, has become a symbol of Italy's anti-death penalty stance. Since 1999, the monument has been bathed in golden light every time a death sentence is commuted somewhere in the world or a country abolishes capital punishment.

"I hope there will be such an occasion soon," Rome Mayor Walter Veltroni said. "When it happens, we will do it with a special thought for Tookie."

Want to make a trillion dollars? Challenge any Eurosavge to name Stanley "Tookie" William's victims, and if they can't, they need to repay all that Marshall Plan money back, with interest.



Albert Owens





Tsai-Shai Yang

Ye-Chen Lin

Why are you so intolerant of other people's cultures?

Gang Rapist Blames Culture

December 9, 2005 – From: www.heraldsun.news.com.au

By Kim Arlington

A CONVICTED gang rapist has told a Sydney court he sexually assaulted a 14-year-old girl because he thought she was promiscuous and "had no right to say no." The 27-year-old, identified only as MSK, said voices had commanded him to rape the girl, but also blamed cultural differences for the attack.

MSK, convicted of raping two girls aged 13 and 14, faced sentencing submissions today before NSW Supreme Court Justice Peter Hidden.

He is already serving a 22-year jail term for leading his three younger brothers in the gang rape of two more girls, aged 16 and 17.

All four attacks took place at the brothers' Ashfield home, in Sydney's inner-west, in June and July 2002.

The court was told the first rape, that of a 14–year–old girl known as T, took place four days after MSK arrived from Pakistan.

MSK took an oath on the Koran before telling the court his cultural background was partly to blame for his crimes.

T, who had visited his house with two female friends, was not wearing traditional Muslim dress, he said.

"She was not covering her face or wearing any headscarf," MSK said.

"Then she started drinking with us ... at one point she started touching my leg."

MSK agreed T had not consented to sex but said: "I go ahead with it because ... I believe that she was promiscuous."

"I believed at the time I committed this offence that she had no right to say no," he said.

"I believed I'm not doing anything wrong."

T had told the trial that before she was raped by MSK and his younger brother MAK, who also was convicted, she was a virgin and had never kissed a boy.

MSK said he believed that his 13-year-old victim, known as C, also was promiscuous.

Now 18, T shook her head as she listened from the public gallery, supported by C's mother.

MSK had visited Australia nine times, including a 10–month stint when he worked as a security guard, before his arrest.

He told the court he now had a "better idea and understanding of Australian culture" after being exposed to the country's media.

"I understand now that what I did at the time was wrong and (that) what I believed was wrong," he said.

MSK also said he was drunk at the time of the offences, and was not taking the anti-psychotic medication prescribed for him by his father, a doctor.

"I was not taking my medication so I was under the influence of voices," he said.

"I was commanded by voices to go ahead."

Crown prosecutor Ken McKay told Justice Hidden that MSK's explanation for the offences kept changing.

"One minute it's the voices, the next minute it's a cultural issue," he said.

Mr McKay said the question of mental illness was raised only this year when MSK's applications to adjourn his trial were refused, but a jury found him fit to be tried.

MSK apologised to his victims for the first time today, but interrupted his apology to tell T: "Don't shake your head – I'm telling you something."

Outside court, T rejected his apology.

"It wasn't a sincere apology. I don't accept it at all," she said.

MSK will be sentenced next year.

Now, lets see what the Chinese are using those illegal Eurosavage weapons for...

















Response from Eurosavages : Silence Response from Amnesty International : Silence Response from Digg Posters : Silence Response from Slashdot Posters : Silence Response from any Hippies : Silence Response from Cuba : Silence Response from Today's "Hackers" : It's all Bill Gates' fault! Response from Canada :

Were cops all wet? CALGARY – A father is demanding an apology from police after he says he was tasered for chasing down a man who had urinated on his I2-year-old daughter. Darcy Boettger said he and his family from Stettler, Alta., were in Calgary at a wake for his wife's brother when a drunken man began to empty his bladder on the young girl and later take aim at her mother. When offices arrived, they went after the huge, furious father, rather than the cowering drunk.