JAERI-Tech
99-041

DEVELOPMENT OF AUTHENTICATION SYSTEM FOR THE FAST CRITICAL ASSEMBLY (FCA) PORTAL MONITOR (P/M) AND PENETRATION MONITOR (PN/M) SYSTEMS OF JAERI

May 1999

Hironobu OGAWA and Takehiko MUKAIYAMA

日本原子力研究所
Japan Atomic Energy Research Institute

本レポートは，日本原子力研究所が不定期に公刊している研究報告書です。

入手の問合わせは，日本原子力研究所研究情報部研究情報課（〒319－1195 茨城県那珂郡東海村）あて，お申し越しください。なお，このほかに財団法人原子力弘済会資料センター（〒319－1195 茨城県那珂郡東海村日本原子力研究所内）で複写による実費頒布をおこなっております。

This report is issued irregularly.

Inquiries about availability of the reports should be addressed to Research Information Division, Department of Intellectual Resources, Japan Atomic Energy Research Institute, Tokai-mura, Naka-gun, Ibaraki-ken 〒319－1195, Japan.

編集兼発行　日本原子力研究所

Development of Authentication System for the Fast Critical Assembly (FCA) Portal Monitor (P/M) and Penetration Monitor (PN/M) Systems of JAERI

Hironobu OGAWA and Takehiko MUKAIYAMA+

Department of Fuel Cycle Safety Research
Nuclear Safety Research Center
Tokai Research Establishment
Japan Atomic Energy Research Institute
Tokai-mura, Naka-gun, Ibaraki-ken

(Received April 6, 1999)

The advanced comprehensive containment and surveillance system for the Fast Critical Assembly facility (FCA) of the Japan Atomic Energy Research Institute (JAERI) consists of a Portal monitor (P/M) and a Penetration Monitor (PN/M) systems. The development of these systems was completed in 1988 for alleviating the burdens of manpower and radiation problems in the frequent NDA inspections.

After the completion of the field trial test (Phase Ⅲ), in 1990, the International Atomic Energy Agency (IAEA) accepted the system on condition that an independent IAEA authentication equipment would be provided.

The development of the authentication measures was carried out jointly by both the Japan Support Programme for Agency Safeguards (JASPAS) and the U.S. Program of Technical Assistance to IAEA Safeguards (POTAS), and also under the research agreement for the safeguards research and development between JAERI and the US Department of Energy (USDOE).

The concept and design requirements of the authentication system were developed by IAEA, but the design and development of the authentication equipment were jointly funded both by JASPAS and POTAS, and also the fund of JAERI was provided for the Sandia National Laboratories (SNL) through USDOE.

SNL developed and constructed the authentication system in two phase as Phase I

+ Center for Neutron Science

and PhaseⅡ. JAERI financed the development of the Phase I and PhaseⅡhardware and software, and the installation of the authentication equipment at the FCA facility, and also carried out the modification of the circuitry and devices for both the P/M and the PN/M systems as well as the reconstruction of the PN/M Junction Unit for compatibility with the implementation of the authentication measures.

After the completion of consecutive field trial test of the P/M, the PN/M and the authentication system, IAEA accepted the entire system as an effective and efficient routine inspection measures in 1996.

This report describes the modification and reconstruction of both the P/M and the PN/M systems by JAERI for full compatibility with the implementation of the authentication system, and also presents both the entire authentication system and its field tests.

Keywords: Authentication, FCA, Fast Critical Assembly, Containment, Surveillance, C/S System, Portal Monitor, Penetration Monitor, Inspection, Safeguards

JAERI - Tech　99 - 041

高速炉臨界実験施設のポータル・モニターとペネトレーション・モニターの
オーセンティケーション・システムの開発

日本原子力研究所東海研究所安全性試験研究センター燃料サイクル安全工学部
小川　弘伸　・　向山　武彦+

（１９９９年４月６日受理）

日本原子力研究所 (JAERI) の高速炉臨界実験装置施設（FCA）の先進的統合型封じ込め・監視システムは、ポータル・モニターとペネトレーション・モニターの２つの相互に補完するシステムで構成されている。本システムの開発は１９８８年に完了し、国際原子力機関 (IAEA) による非破壊測定分析（NDA）を主要な手段とする頻繁な査察に伴う人的資源の負担や放射線被曝の軽減を当初の目的とした。１９９０年に IAEA は、長期間に亘る予備現地試験（第３期）を終了し、保障措置目標を達成するシステムとして受け入れた。但し、IAEA は、本システムのデータ真正性の担保手段として、IAEA の独立したオーセンティケーション装置の具備を条件とした。

オーセンティケーション・システムの開発は、日本の対 IAEA 保障措置技術開発支援計画 (JASPAS) と米国の対 IAEA 保障措置技術支援計画 (POTAS) 、及び JAERI と米国エネルギー省 (DOE) との保障措置研究協力協定の下で行った。

IAEA はオーセンティケーションの概念及びシステム設計必要条件の提案・開発を行い、オーセンティケーション機器の開発は、JASPAS と POTAS との共同の資金負担により実施された。また、JAERI 負担分は DOE を通じて米国サンディア国立研究所 (SNL) に提供された。

システムの開発は、SNL が２期に分けて実施した。JAERI は、この２期に亘るハードウェアとソフトウェアの開発に係わる資金を負担すると共に、開発における技術支援と本システムの設置及びこれに伴うポータル、ペネトレーション・モニターの改造を実施した。

ポータル・モニター、ペネトレーション・モニター及びオーセンティケーション・システムの長期に亘る入念な予備現地試験を終了後、IAEA はこのオーセンティケーション・システムを効果的・効率的な通常査察措置として１９９６年に受け入れた。

本報告書は、オーセンティケーション・システムの開発において、日本原子力研究所が実施した内容を主として、開発とその進展、それに係わるフィールド・テストとその結果及びシステム全体の理解が出来るように詳述した。

東海研究所：〒３１９－１１９５　茨城県那珂郡東海村白方白根２－４
+中性子科学研究センター

This is a blank page.

Contents

目　　次

A List of Figures

A List of Photos

1. Introduction

The Fast Critical Assembly facility (FCA) of the Japan Atomic Energy Research Institute (JAERI) at Tokai in Japan is considered as one of the most sensitive facilities from the viewpoint of the safeguards[1]. Therefore, safeguards inspection activities executed by the International Atomic Energy Agency (IAEA) were very frequent, then the development of the advanced comprehensive Containment and Surveillance (C/S) system for FCA was begun in 1979 for alleviating the burdens of manpower and radiation problems in those inspections. This FCA C/S system consists of both the Portal Monitor (P/M) and the Penetration Monitor (PN/M) systems [1,2].

After the completion of the construction for the system, the field trial test (Phase Ⅲ) was conducted from December 1988 to June 1989. On the one hand, in September 1988 the authentication proposal letter had been sent from H.Kurihara (IAEA, SGDE) to H.Tani (Japan Nuclear Safety Bureau, JNSB) in July 1988. After that, the authentication project was initiated with the letter that was sent from J.Jennekens (IAEA, DDG-SG) to K.Takagi (JNSB) for JASPAS/POTAS collaboration on the authentication development for the FCA C/S System.

The IAEA presented a policy of "Use of operator-provided, installed C/S equipment in IAEA safeguards" in INMM 28th Annual Meeting in July 1987[3]. At this meeting, the IAEA also presented a concept of "Authentication of an operator-provided Containment and Surveillance (C&S) system" [4]. This article describes IAEA considerations for some specific methods of authentication for a pioneering operator-provided FCA C/S system in Japan.

In accordance with above both policy and concept of authentication measures to operator-provided C/S system, the IAEA documented "Specification of the authentication equipment" to be installed at the P/M and PN/M systems in October 1988. According to the specification of the authentication equipment, the Sandia National Laboratories (SNL) designed the authentication equipment in detail during 1989 under the U.S. Program of Technical Assistance to IAEA Safeguards (POTAS). In May 1990, an authentication design review meeting was held at SNL with participants from IAEA, JAERI and SNL, there and then SNL design was approved by all participants [5].

Prior to the authentication design review meeting, in February 1990 the IAEA sent an official letter to JNSB for an approval of the FCA C/S system on condition that an independent IAEA authentication equipment was provided [7,8].

The project of the authentication system was divided into two phase, Phase I and Phase Ⅱ. The Phase I provided the inspectorate with a printed listing of recorded events which must be compared with the records produced by the FCA C/S system. The

Phase I authentication equipment consists of two authentication controllers, a P/M Authentication Controller and a PN/M Authentication Controller [5].

The Phase II provided the authentication equipment records to be automatically compared with the FCA C/S system records by means of a personal computer [6].

The U.S. Program of Technical Assistance to IAEA Safeguards (POTAS) funded the development of the authentication design. SNL provided the IAEA with the authentication equipment including its software in the Phase I and the automatic data comparator in the Phase II. JAERI funded the development of the Phase I and Phase II hardware and software, and also the installation of the authentication system at the FCA facility through the research agreement for the safeguards research and development between JAERI and the US Department of Energy (USDOE), and the entire project of JAERI for the authentication system was carried out under the Japan Support Programme for Agency Safeguards (JASPAS).

JAERI conducted the modification of the circuitry of both the P/M and the PN/M systems as well as the reconstruction of the PN/M Junction Unit itself to install the authentication controller in June 1991.

The three organizations (JAERI, SNL and IAEA) held a meeting on the pre-installation of FCA C/S system authentication equipment in JAERI in August 1991 prior to the provisional installation of the authentication equipment for a preliminary test at FCA in September 1991.

The authentication controllers were delivered to the FCA facility from the SNL in November 1991 and were installed. At the same time the DataKey hardware and software were sent to the IAEA Tokyo Regional Office (TRO) for only use by the IAEA inspector.

The first field test of the authentication equipment was carried out during four periods on the monthly basis from November 1991 to March 1992.

In December 1992, the automatic data comparator software was delivered to FCA from SNL, and at that time a portion of the authentication controller firmware was changed by resulting from the first field test.

The second field test of both the authentication equipment and the automatic data comparator was carried out for four periods from December 1992 to April 1993. As a result of the test, it was agreed that the test would be extended.

The pre-test of both the authentication equipment with the automatic data comparator and the FCA C/S system was executed for commencing the next field test in February 1994. The "phase two" field test as the extended second field test of both the authentication equipment and the automatic data comparator was carried out for four periods from February 1994 to May 1994.

The final field test report of the FCA authentication equipment and the automatic data comparator system only was documented by IAEA in May 1995. It was stated that the system performed well as expected.

Finally, this worthy joint project was successfully completed under the agreement of both JNSB and IAEA in September 1996.

This report presents an outline of the FCA authentication measures and describes the sufficient provisions with both modification and reconstruction of the FCA C/S system, the P/M and the PN/M systems, carried out by JAERI so as to be fully compatible with the implementation of the authentication system.

In the end of this report, several documents relevant to the authentication system provided by SNL under the fund of JAERI are attached as appendixes.

2. Concept of Authentication of Both P/M and PN/M Systems

The P/M and PN/M systems are operator-designed and -manufactured, and are the first fully automatic, unattended, pioneering systems for routine inspection use at the FCA facility of JAERI. The development and installation of the systems was made completely transparent to the IAEA. Because the FCA C/S system was constructed in cooperation with the IAEA through its development and installation [7,8]. However, the FCA C/S system has a precedent nature of potential use for international safeguards. Therefore, the IAEA considered that rigorous standards for authentication should be established. The concept and design requirements for an authentication system were developed and documented by the IAEA [3,4].

To make the FCA C/S system a credible safeguards system, the IAEA required an independent and reliable means of authenticating the data recorded with an operator-provided comprehensive C/S system, and also required to assure the proper functioning of the FCA C/S system.

The IAEA presented three basic goals in accordance with the Agency Authentication Approach as follows :

(1) It must be credible to the Agency and to the international community.

(2) It must have little or no impact on the normal operation of the C/S system.

(3) It must place a minimum of additional burden on operators and IAEA inspectors and maintenance personnel.

The FCA authentication project took place in two phases, Phase I and Phase Ⅱ. The Phase I provided the inspectorate with a printed listing of recorded events which must be manually compared with the record produced by the FCA C/S system. The Authentication Equipment (AE) consists of two authentication controllers, a P/M Authentication Controller (AC) and a PN/M Authentication Controller (AC). Each one produces a record of events compared with each C/S system record during each IAEA inspection period.

The Phase Ⅱ was intended to provide the authentication equipment records to be automatically compared with the FCA C/S system records by means of a personal computer.

The authentication equipment stores passive monitoring sensor events and activation events of critical sensors simulated randomly.

The P/M Authentication Equipment can monitor individually up to three sensors programmed by the IAEA in the P/M system. The metal detector (MD1) of the P/M monitor is the most critical component in the system, therefore the metal detector is always monitored and is also tested randomly by activating from the Authentication Controller through the self test circuit of MD1 as well as to assure its proper operating.

The PN/M Authentication Equipment (AE) can monitor individually up to three sensors selected by the IAEA in the PN/M monitor. The selected those sensors can also be selected, from any one to all one, for a random active testing, but no other sensors can chosen for a random active test.

The recorded event data is tagged with time of day and date, and is stored on a NOVRAM (Non Volatile Random Access Memory) for retrieval by a personal computer of IAEA inspectors. Therefore, the Authentication Controller Clocks must be synchronized with the FCA C/S system clock to facilitate a comparison between the data produced by the Authentication Equipment and the data recorded by the FCA C/S system.

2.1 Authentication Concept of P/M System

The conceptual block diagram of the Portal Monitor is shown in Fig.1. The P/M system consists of three units, the Detection Unit (DU), the Junction Unit (JU) and the Control Unit (CU).

Figure 3 is a conceptual block diagram of the FCA Portal Monitor with the P/M Authentication Equipment (AE) and illustrates how the P/M Authentication Equipment is connected to the P/M system.

The P/M Authentication Equipment at the FCA facility consists of the Authentication Controller (AC), the DataKey which is composed of an EEPROM (Electrically Erasable Programmable Read Only Memory) and the Personal Computer.

The P/M Authentication Controller is located and fixed on the top of P/M Junction Unit as shown in Photo 2, while both the DataKey and the personal computer are brought with IAEA inspectors at the inspection. The Power of P/M Authentication Controller is provided by the P/M Junction Unit under normal conditions, but it will be provided for 3 hours operation through a built-in battery in the case of the P/M system power failure.

The DataKey having the operating parameters of the Authentication Controller is transported from the IAEA Tokyo Regional Office (TRO) to the FCA facility. The operating parameters for both passive and active monitoring are set by the DataKey programming software at the IAEA TRO. Therefore, no one other than IAEA inspectors knows those operatiing parameters.

For the passive monitoring of all sensors of the P/M Detection Unit, those sensors' signals are picked up at the Multiplex Transmitter modules. Those signals are sent to the P/M Authentication Controller through the Isolated Interface Circuitry inside the P/M Junction Unit. The Authentication Controller Clocks are fed independently by the CPU of the P/M Control Unit through the Multiplex Transmitters of both the P/M Control Unit and the Junction Unit.

For the active monitoring of Metal Detector (MD1) activation, the trigger signals for MD1 activation by the P/M Authentication Controller are connected directly from the P/M Authentication Controller into the check circuit of the MD1.

2.2 Authentication Concept of PN/M System

The conceptual block diagram of the Penetration Monitor is shown in Fig. 2. The PN/M system consists of two units, the Junction Unit and the Control Unit.

Figure 4 is a conceptual block diagram of the FCA Penetration Monitor with the PN/M Authentication Equipment and illustrates how the PN/M Authentication Equipment is connected to the PN/M system.

The PN/M Authentication Equipment at the FCA facility consists of the Authentication Controller, the DataKey and the personal computer. The hardware configuration of the PN/M Authentication Equipment is very similar to the one of the P/M Authentication Equipment. The P/M Authentication Controller however, has two metal detector test buttons and one more isolated I/O board than the PN/M Authentication Controller. Conversely, the P/M Authentication Controller software is quite different from the PN/M Authentication Controller software.

The PN/M Authentication Controller is installed inside the PN/M Junction Unit as shown in Photo 5. Both the DataKey and a personal computer are carried by IAEA inspectors at the inspection. The PN/M Authentication Controller Power is provided by the PN/M Junction Unit under normal conditions. However, the Authentication Controller provides a continuos operation for three hours by an internal battery at the time of the PN/M system power failure.

The DataKey included the operating parameters of the PN/M Authentication Controller is brought from the IAEA TRO to the FCA facility. The operating parameters for both passive and active monitoring are set exclusively by the IAEA inspecters at the IAEA TRO. Therefore, no one other than IAEA inspectoers knows the operating parameters.

For the passive monitoring of all infrared motion sensors at both the Reactor Room (inside Inner Building of reactor container) and the Annulus (inside Outer

Building of reactor container), those sensors' signals are sent to the PN/M Authentication Controller via the Terminal Blocks and through the Isolated Interface Circuitry inside the PN/M Junction Unit. The PN/M Authentication Controller Clocks are fed independently by the CPU of the PN/M Control Unit through the Multiplex Transmitters of both the PN/M Control Unit and the PN/M Junction Unit.

All infrared motion sensors of the PN/M system at both the Reactor Room and the Annulus are monitored actively. The active signals for the those sensors' activation by the PN/M Authentication Controller are joined individually with those sensors outputs at the Terminal Block, and also are fed to the PN/M Control Unit through the Multiplex Transmitters of both the PN/M Junction Unit and the PN/M Control Unit.

3. Outline of Authentication System

The FCA Authentication System records the activation events of selected sensors and compars lately this record with the FCA C/S system record. The Authentication Equipment initiates random tests of selected sensors, and as a result, those sensor activation can be recorded by both the FCA C/S system and the Authentication Equipment.

The FCA Authentication System consists of the Authentication Equipment , its relevant software and the Automatic Data Comparator.

The Authentication Equipment consists of the following several hardware and several software.

Hardware

(1) Portal Monitor Authentication Controller with Embedded Software

(2) Penetration Monitor Authentication Controller with Embedded Software

(3) Loop back connectors for a self diagnosis between the computer and the Authentication controller

(4) DataKey Interface Module with power adapter

(5) DataKeys (EEPROM)

(6) RS232 serial communication cable between the computer and the Authentication Controller

(7) Fully IBM compatible personal computer with battery backup

(8) Printer with cables and papers

(9) 3.5 inch 720KB or 1.44KB floppy disk

Software

(1) ONSITE Software (“**Onsite**”)

(2) DataKey programming Software (“**ProgdKey**”)

(3) Automatic Data Comparator Software (“**FCAcomp**”)

The P/M and the PN/M Authentication Controllers provide with the following outstanding features in common.

(1) It provides passive monitoring capabilities and randomly simulates activation of critical sensors.

(2) It records data tagged with time of day and date, and store this information on a Non Volatile Random Access Memory (NOVRAM) for retrieval by an IAEA inspector by means of a personal computer.

(3) Clocks of the authentication controller are synchronized with the FCA system clock to facilitate a comparison between the data produced by the authentication equipment and by the FCA C/S system.

(4) It is capable of a continuos operation for three hours by an incorporated battery at that time of a power failure of the FCA C/S system.

(5) The connections between the Authentication Controller and the operator's equipment are isolated by the use of optical isolators and relays as Input/Output Interface Circuitry to avoid interference with normal operation of the FCA C/S system.

(6) The enclosure is made of anodized aluminum to provide a tamper indication and its cover can be secured with seals of both authorities, the IAEA and JNSB (see Photo 1).

(7) The enclosure exterior is featured with a DataKey receptacle and an RS232 communication port (see Fig. 34).

(8) The operating parameters can be programmed individually by means of a portable EEPROM (Electrically Erasable Programmable Read Only Memory) DataKey.

3.1 Authentication Equipment (AE)

The Authentication Equipment consists of two Authentication Controllers and other equipment mentioned above.

The exterior and outside dimension of the Authentication Controller is shown in Photo 1 and Fig. 34.

The Authentication Controller is a key component of the Authentication Equipment and consists of several functional boards and modules. These are Power Supply, Microprocessor Board, I/O Expander Board, Isolated I/O Board, Clock Interface Board, DataKey Interface Board, Nonvolatile Read/Write Memory Cartridge and PC Interface.

Power Supply

The AC power input is universally 90 – 250 V AC and 44 – 440 Hz, and the

DC power output is 5 V DC @4 A and 12 V DC @0.5 A. 5 V DC output is used for normal system operation and 12 V DC output charges the battery. This battery is an 8 V, 3 A–hour, lead-acid battery.

A Power Supply board monitors external power, maintains the charge of battery and turns on the battery output to the controller circuitry at the time of AC power loss.

Microprocessor Board

The microprocessor unit is available in commercial, but was slightly customized to address the 500K-Byte NOVRAM memory module. An address decoder was provided for this purpose and three additional address lines was attached to the decoder chip socket. The microprocessor board is configured for a specific application by installing jumpers.

The embedded software resides on a 64K-EPROM and operates each Authentication Controller.

I/O Expander Board

An Input/Output Expander board extends the I/O capabilities of the system and permits several isolated I/O boards to be addressed by the system.

Isolated I/O Boards

The design concept of the authentication system is to isolate electrically all signals between the Authentication Equipment and the FCA C/S system. These isolated I/O boards are used to optically isolate sensor inputs to the Authentication Equipment and to isolate all outputs by relays to the FCA C/S system.

Clock Interface Board

Time of day and date signals from the FCA C/S system are transmitted to the Authentication Equipment on 31 inputs through the clock interface board. The clock interface board is a custom-designed board that provides optical isolation and decoding functions of the signals.

DataKey Interface Board

The data communication between the DataKey interface circuitry and the microprocessor is done through the RS232 channel of the Microprocessor Board.

Nonvolatile Read/Write Memory Cartridge (NOVRAM)

The Nonvolatile Read/Write Memory Cartridge has an internal battery to keep the stored data, but the battery has an expected life of five years from the manufactured date.

PC Interface

The communication for the operation of the Authentication Controller (AC) is done through the RS232 connector of the AC and the communication cable by using the inspector's computer.

DataKey

The DataKey is an EEPROM device, and stores the operating parameters of either the P/M Authentication Controller or the PN/M Authentication Controller on the one of two DataKeys by an IAEA inspector at the IAEA TRO before leaving to the FCA facility.

The purpose of the DataKey is to provide a secure and rugged means of transporting the operating parameters of the Authentication Controller to the FCA facility.

At the IAEA TRO, the DataKey is programmed by using together with an exclusive software (**ProgdKey**) in the IAEA inspector's personal computer and DataKey Interface Module.

At the FCA facility, the DataKey is used together with a software (**Onsite**) in the IAEA inspector's personal computer connected to the Authentication Controller and then the Authentication Controllers can be reprogrammed. However, neither the DataKey nor the computer alone can be used to change the operating parameters of the Authentication Controller.

3.2 Onsite Software

In addition to the embedded programs in the Authentication Controllers, two software programs, **Onsite and ProgdKey**, are provided by the IAEA, and each one operates on IBM compatible personal computers provided by the IAEA.

Onsite Program

The Onsite Program permits a communication to set the new operating parameters with the Authentication Controllers, also to commence and quit its data acquisition, and to download stored data to the IAEA inspector's computer and to usually 3.5 inch floppy disk of its computer.

The Onsite Program can operate from either "On-Site Service Diskette" or the computer Hard Disk which is already installed the program.

When the Onsite Program is initially run on a laptop computer, the title screen appears firstly and the operator can check or change the current time of day and date. After that, the Onsite program displays the Main Menu with the current time and date.

Main Menu

The Main Menu of Onsite Program consists of "Controller Services", "Diskette Services", "Report Generation", "Loop-Back Test" and "Quit to DOS".

Controller Services

This menu initiates a communication between the computer and the Authentication Controller. This program identifies the controller (P/M or PN/M) or warns the operator that communication cannot be established. After the communication is established and the controller is identified, either the **P/M or PN/M Authentication Controller Menu** appears. While the communication is established with an Authentication Controller that is now in operation and acquisition, that acquisition period accomplishes and the current time and date are recorded.

Diskette Services

This menu is utilities that allow the inspectors to format diskettes properly for use as either the P/M or the PN/M Authentication Controller. These data diskettes can be checked to identify the data on a diskette that might be used as either data diskette.

Therefore, the Authentication Equipment can check and maintain the identification of data during the report generation process.

This menu consists of the following options.

Lists files

This option checks the diskette and reports the disk contents to the inspectors.

Format a Portal Data Diskette

Format a Penetration Data Diskette

Quit to Main Menu

Report Generation

This program permits the inspectors to select an acquisition record of interest, clock synchronization data or self test data from a data diskette. All recorded data can be reviewed on the computer display or printed.

When the system detects a valid data diskette in the disk drive, this Report Generation Menu displays the following functions.

Choose Drive For Files

This program indicates you to enter the letter of a disk drive or a RAM drive with at least 2 megabytes of available memory space.

Viewing Data

While the data is displaying in "scrollable region" on the display, the inspectors can see the paginal data by using the cursor arrow keys to scroll up, down and sideways, and may also print the data in the Report Menu by using the ALT/P keys and the ESC key to quit.

Acquisition Data

When the data is downloaded to a data diskette from an Authentication Controller, the acquisition data is stored in a file that is identified. The file data contains the date of a started acquisition period and a sequential number of the file.

The acquisition data can also be sorted in detail by choosing **Sort List Options**.

Report Format

The acquisition data is indicated in a report with seven columns of information. Those column headings consist of "Event", "Event time", "Status", "Test, EOM (End of Memory)", "Time>2" and "MD Test".

- Event -

An event shows the designation for a sensor or a condition that recorded during an acquisition period. Some event designations in the Authentication Equipment are particular to the FCA C/S system which do not assign those designations.

- Event time -

This is the time when an event occurrence and the record is accomplished when a sensor activation began and ended.

- Status -

An "ON" indication appears in this status column while a sensor activates, and an "OFF" marks at the end of its activation.

- Test -

This column is marked with a "Test" when a test by means of the authentication equipment initiates.

- EOM -

EOM is marked on the last event record stored just before the nonvolatile memory (NOVRAM) had no space to store. Even if any events occur after that, no event record is stored on the memory until the End of Acquisition.

- Time>2 -

"Time>2" means that YES is displayed in the column, When the time difference between the FCA C/S system and its Authentication Equipment is greater than 2 minutes for an event.

- MD Test -

When a metal test is initiated, this column is filled with the reason for the test, namely TIME or PERCENT.

Clock Data

The inspectors can view the clock data or print a hard copy to examine the time difference between the two clocks, both clocks of the Authentication Equipment and the FCA C/S system, before synchronization and to verify synchronization at the commencement of an acquisition period.

Self Test Data

Whenever the Authentication Equipment performs a self test, the test results are always stored in a self test file on the data diskette. The results of each self test are displayed with the time and date of the test.

Quit to Main Menu

Return to the Main Menu of the Onsite Program.

Loop-Back Test

This option is a trouble shooting aid as a diagnosis for the event of a communication trouble between the computer and the Authentication Equipment. This program is used together with a loop-back connector, and also is used to identify a problem of communication function on the computer, the communication cable or the Authentication Controller, individually.

Quit to DOS

This option is to exit the Main Menu of Onsite Program and to return control to the computer operating system.

P/M or PN/M Authentication Controller Menu

These menus consist of “End of Acquisition Period”, “Download Acquisition Data to PC”, “Program Authentication System Parameters”, “Start Acquisition Period”, “Controller Self Test” and “Quit to Main Menu”.

End of Acquisition Period

This program stops a data acquisition of the Authentication Controller and records the date and time that the acquisition ended. Just after an acquisition period started, this option can also quit it.

Download Acquisition Data to PC

This program interrogates the Authentication Controller to determine the file size required and checks that information about the available storage space on the data diskette. The program also checks if a data diskette is properly inserted into the disk drive or not, and if the inserted diskette is properly formatted or not. After these checks completed, the program transfers the data stored in the Authentication Controller to the data diskette.

Program Authentication System Parameters

A programming of the system parameters to the Authentication Controller needs to use a DataKey together with an inspector's personal computer. The system parameters of the Authentication Equipment cannot be reprogrammed during the data acquisition. Therefore, the acquisition should not be commenced until the new parameters are set into the Authentication Controller.

Start Acquisition Period

The Authentication Equipment synchronizes the Authentication Controller Clock with the FCA C/S System Clock. At this time, the proper data diskette should be in the disk drive of the computer because the clock data is stored on it. Both clock times are stored before and after the clock synchronization and these data are displayed on the computer monitor.

When the clocks of the Authentication Equipment have been successfully synchronized and the clock data has been transferred to the data diskette, the Authentication Equipment begins to monitor and stores data according to the operating parameters loaded into the system.

While the acquisition begins, the data in the Authentication Equipment Memory is cleared and the stored data is lost unless the data has been downloaded. Consequently, the previous acquisition data should be downloaded to a data diskette before commencing a next acquisition period.

Controller Self Test

The Authentication Controller has a self diagnosis function that can operate when the controller is not in acquisition. The self diagnosis function of the P/M

Authentication Equipment is different from the one of the PN/M Authentication Equipment, then the self tests themselves are also different. Each self test procedure takes about two minutes. Both self tests diagnose the system memory (RAM) and a non-volatile memory cartridge (NOVRAM), and those results are indicated on the computer display and are also stored on the data diskette. Each Authentication Controller has the following unique self test features.

P/M Authentication Controller Self Test

The self test does not activate the infrared sensors. If the independent self test of the Metal Detector functions is necessary, Two push-buttons inside the Authentication Controller can activate the Metal Detector (MD1) self test function. The two buttons are labeled MD1-A and MD1-B respectively and actuate each self check circuitry in the MD1.

PN/M Authentication Controller Self Test

The self test interrogates the Authentication Controller's capability to trigger individual sensor relays of the PN/M System and to read the resulting simulated sensor activation. Therefore, each sensor relay is sequentially activated and read it again on condition that nobody is within the sensitive zone of all motion sensors in the reactor room and the annulus area of the reactor building.

Quit to Main Menu

This is to return back to the On-Site Services Main Menu.

Sort List Options

Sort List

When the "Acquisition Data" had already been selected from the Report Generation of **Main Menu** and a data file was chosen, a Sort List displays. The options perform to sort the data file three different ways, namely "Single Sensor", "Sensor ID" and "Chronological", and display the sorted data in a scrollable region of the computer monitor or print all data specified.

Single Sensor

This option chronologically sorts all events associated with the sensor of interest.

Sensor ID

This option chronologically sorts and groups the events according to the sensor identifications

Chronological

The event data is presented in the same order as it was accumulated. All events recorded during an acquisition period are included.

3.3 ProgdKey Software

The ProgdKey program is used at the IAEA TRO to set the operating parameters of the Authentication Equipment on the DataKey memory device. This software is provided with one 3.5 inch floppy disk to program the DataKeys with both a DataKey Interface Module and a personal computer.

Main Menu

The Main Menu of the software consists of three options, namely the Portal Monitor option, the Penetration Monitor option and the Quit to DOS option.

One DataKey has a capability of storing the operating parameters for both the Authentication Controllers. Therefore, if one DataKey has already stored the operating parameters for one of the Authentication Controllers (P/M or PN/M), the Main Menu is fixed its selection to the remaining option. When starting up the software to load any operating parameters on the DataKey, the software automatically initializes and erases all information stored previously.

Portal Monitor option

The P/M Authentication Controller can passively monitor 0 to 3 sensors in the P/M system in addition to the random test of the Metal Detector (MD1). The sensor choices for a passive monitoring are provided with the following selections.

- The number of sensors to passively monitor
- The identification of sensors to be monitor according to selected number
- The way of random active testing to the Metal Detector

The Metal Detector may test randomly based on a percentage of occupancies inside the MD1 and/or a time interval. To eliminate this test mode, simply type zero.

Penetration Monitor option

At first, an inspector must select the number of sensors monitored by the PN/M Authentication Controller. The PN/M Authentication controller can passively monitor up to three sensors and actively monitor those sensors at random time base, but this active monitoring simulates sensor activation in contrast to the real active tests of the Metal Detector (MD1).

Quit to DOS option

The inspectors can return any time to the Main Menu, and to computer operating system.

3.4 Automatic Data Comparator

The Automatic Data Comparator is a software usesd with the Authentication Equipment at FCA. The software is provided on one 3.5 inch diskette and is installed in a personal computer to enable an inspector to perform a data comparison. For use by the Automatic Data Comparator, a fully IBM compatible computer with a hard disk or a 2MB RAM drive is required.

The Automatic Data Comparator named **FCAcomp** is the program that makes a comparison between both the P/M or the PN/M authentication data and the data recorded by the P/M or the PN/M equipment, respectively.

The Operating Instructions of the Authentication Data Comparator

Set Date and Time

When the FCAcomp program commences to run, a title screen appears and the inspectors can verify or correct the date and time of day information.

Disk Space Check

After the date and time is set correctly, the FCAcomp program examines a drive " C " to determine if at least 2 Megabytes of disk space is available for temporary files. If there is insufficient space on the drive C, the inspectors are required to identify a disk drive or a RAM drive that the FCAcomp software can use.

Insert Authentication Data Diskette

After the FCAcomp program sets up a scratch area as a drive for temporary files, it prompts the inspectors to insert a data diskette of the Authentication Equipment into the disk drive.

File Display

The FCAcomp software reads the authentication data diskette and displays all files on the diskette. After the FCAcomp program duplicates the chosen file to the scratch area, the program prompts the inspectors to remove the authentication data diskette from the disk drive.

Insert FCA C/S data diskette

After the authentication data diskette removed from the disk drive, the program asks the inspectors to insert an FCA C/S data diskette into the disk drive.

Program Results

After the FCA C/S data files are copied from the diskette, a program prompt shows the inspectors to remove the diskette. The FCAcomp software compares the data of the two diskettes and then indicates the results of comparison. The program can print the records and the maximum 800 unmatched events as a result of the data comparison, but not show the entire listings on the computer display.

Exit

After the unmatched events are presented, the execution of the FCAcomp program is completed. Exit the program by pressing the ESC key.

Alert Messages

While the comparison of the two data diskettes is completed, the unmatched events present in a scrollable region on the computer display. A highlighted alert message appears in the above or below scrollable region under three conditions as the followings.

There were records that have a time difference of greater than 2 minutes !

The automatic data comparator software found the events that had a " Time>2 " flag in the authentication record.

An End of Memory condition occurred during this reporting period !

The nonvolatile memory cartridge in the Authentication Controller filled up during the inspection period. No data was recorded after the event with this flag.

There are more records in the file than can be displayed !

Approximately 800 unmatched events can be displayed in the scrollable region on the computer screen. To watch the complete listings of unmatched events, the inspectors must print out the event records.

3.5 Notices on System Maintenance

The SNL gave notices the following two matters on the maintenance of authentication system.

(1) Two components of the Authentication Controllers, the nonvolatile memory (NOVRAM) cartridge and the backup battery, should be

replaced by the end of their lifetime. These components have a minimum life expectancy of five years.

(2) The software corrections should be made to the authentication system prior to the year 2000.

(Each EPROM of both the P/M and the PN/M Authentication Controller has already replaced with new ones to cope with a problem of 2000 calendar year in August 1993.)

4. Description on Modification of Both P/M and PN/M Systems

For the installation of the Authentication Equipment at the FCA facility, JAERI carried out the modification of several circuitry to both the P/M and the PN/M systems as well as the reconstruction of the PN/M Junction Unit for fully compatible with the implementation of the authentication system.

JAERI carried out the following five major things to install the two Authentication Controllers to each Junction Unit of both the P/M and the PN/M systems.

(1) The transmission of the system clock (Date and Time of Day) from the FCA C/S system clock to the Authentication Controller clock.

(2) The connection of all sensors' output signals monitored by the Authentication Equipment, and also output signals to both the Metal Detector of the P/M system and all Space Sensors of the PN/M system that subject to actively monitor and test by means of the Authentication Equipment.

(3) The provision of Power Supplies in both the P/M and the PN/M Junction Unit for both the P/M and the PN/M Authentication Controller, the Isolated Input/Output Interface Circuitry and also the Clock circuitry.

(4) The reconstruction of the PN/M Junction Unit to contain the PN /M Authentication Controller inside its Junction Unit in compliance with the IAEA requirement.

(5) The modification on the system software both the P/M and the PN/M systems for dealing with the system clock as mentioned in the item (1) above.

The P/M Authentication Controller is installed at the top of the Junction Unit of the P/M System as shown in Fig. 5 and Photo 1 to Photo 3. The PN/M Authentication Controller is installed inside the new Junction Unit of the PN/M System as shown in Fig. 24 and Photo 5. The identical housing of the Authentication Controller both the P/M and the PN/M Systems is shown in Fig. 34 and Photo 1. The PN/M Junction Unit constructed newly is shown in Fig. 24, Photo 4 and Photo 5.

The modification of the system software of both the P/M and the PN/M systems was carried out to handle the transmission of the system clock from the P/M and the PN/M systems to the P/M and the PN/M Authentication Controller, respectively. But no other modification of the original system software was carried out.

4.1 Detailed Modification of P/M System

4.1.1 Transmission of System Clock from P/M System to P/M Authentication Controller

The recorded event data of the P/M Authentication Controller should be tagged with the time of day and date information to facilitate a comparison between the data of the PN/M Authentication Controller and the data of the P/M System. Because the Automatic Data Comparison will verify a time discrepancy of between the identical event data caused by both the P/M Authentication Controller and the P/M System. Then, both the P/M Authentication System and the P/M System have to have the same time of day and date for an event in principle. Therefore the P/M System sends the time of day and date information to the P/M Authentication Controller. The clock information consists of Second, Minute, Hour of day, Day of month and Month of year, but the year of calendar. Only last 2 digits of the calendar year are set to the P/M Authentication System through the personal computer for inspector.

The modification of the P/M System for this purpose was carried out by JAERI. The conceptual diagram of the Portal Monitor is shown in Fig. 1. This conceptual diagram is for the original entire system before the installation of the authentication system. After the installation of the P/M Authentication Controller, the block diagram of both the FCA P/M System and the P/M Authentication Equipment is shown in Fig. 3. The P/M Authentication Equipment at the facility consists of the P/M Authentication Controller, the P/M DataKey and the Inspector Personal Computer.

The clock signal of the P/M System is transmitted to the P/M Authentication Controller via the I/O interface circuitry of the P/M System's CPU and the Multiplex Transmitter Devices (Data Trans) of both the Control Unit and the Junction Unit through the optical fiber cable.

The modification of the system is described hereinafter in down flow manner for the clock signal from the P/M System's CPU to the P/M Authentication Controller.

As illustrated in Fig.10, one Output Interface Board (OUT 7) is newly provided with the I/O Interface Unit of the CPU, and the output signals of the clock from the CPU are sent to the multiplex transmitter of the P/M Control Unit. The total of six modules (Data Trans) are installed at both the Control Unit and the Junction Unit, three Transmitter modules (GDT) at the Control Unit and three Receiver modules (GDL) at the Junction Unit, respectively. Those modules are shown in Fig. 5 and Fig. 6.

The detailed connection of the clock signals from the P/M CPU I/O Interface board to the Multiplex Transmitter modules is shown in Fig.12 and the detailed connection of those one from the multiplex transmitter Modules to the I/O interface circuitry of the P/M Authentication Controller is shown in Fig. 13 and Fig. 14. The clock signals composed of Month, Day, Hour, Minute and Second are sent as mentioned above.

The clock interface circuitry of the P/M Authentication Controller provides the optical isolation and the data decoding functions, so that the input signals of clock information in the P/M Authentication Controller are completely isolated from those in the P/M systems electrically.

4.1.2 Connection of All Sensors' Output Signals Monitored by P/M Authentication Equipment

The Space Sensors, the Beam Sensors, the Equipment/Emergency Door Switch and the Metal Detector are monitored by the P/M Authentication Equipment. Therefore, the outputs of those sensors should be connected to the P/M Authentication Controller.

As shown in Fig. 3, those outputs are divided into two directional connection at Terminal Blocks for the Multiplex Transmitter Modules of the P/M JU. At the Terminal Blocks, the one is connected to the inputs of the Multiplex Transmitter Devices and the other is wired to the Input/Output Interface Circuitry of the P/M Authentication Controller via the Isolated I/O Interface Circuitry that completely isolates the electrical signals of the P/M System from the one of the P/M Authentication Controller.

The parts' configuration on the Isolated I/O Interface Circuitry board is shown in Fig. 8. The ten couples of Input/Output circuitry of this board is shown in Fig. 9. In this board, the input electrical signals are changed to the dry relay contact signals as the output signals.

Four Isolated I/O Interface Boards are provided with the interface circuit shelf on the new Interface Board Panel inside the JU of the P/M as shown in Fig. 7. This panel is also provided with the Power Supplies and their switches for the P/M Authentication Equipment. The circuitry of Power Supplies provided newly is shown in Fig. 11.

The detailed connection of the Space Sensors, the Beam Sensors, the Metal Detector and the Equipment/Emergency Door Switch to the P/M Authentication Controller through the Isolated I/O Interface Circuitry is shown in Fig. 18 to Fig. 23. As illustrated in Fig. 22 and Fig. 23, the Metal Detector has four output signals, those are the Metal-Detected (5V threshold level) and the Metal-Detected-High (10V threshold level) for both the XY and the Z axial amplifiers, respectively.

The above sensor signals are optically isolated again by the I/O interface circuitry of the P/M Authentication Controller.

4.1.3 Connection for Active Output Signals of P/M Authentication Controller to Metal Detector

The Metal Detector (MD1) included two controllers is the main component of the P/M System and is designed to detect the transfer of a single 2 inches x 2 inches x 1/16 inches fuel coupon in any orientation and at any location through the P/M system. The MD1 is also provided with a self-test circuit which effectively checks out the state of health for the entire metal detector system during every P/M System start-up. Although the MD1 has a self-test function by the system CPU, each Metal Detector Controller provides a push button switch inside its Controller for a manual check at the place.

For monitoring of Metal Detector (MD1) activation, the trigger signals of the P/M Authentication Controller to the MD1 are directly connected from the P/M Authentication Controller into the two Metal Detector Controllers, the MD1A for the XY-Axial and the MD1B for the Z-Axial respectively, as shown in Fig. 17.

The System Block Diagram (X-Y Axial) of Metal Detector (MD1) is illustrated in Fig.15. The check circuit of active signal for monitoring of the MD1A is newly provided with the MD1A circuitry in addition to the proper self-test circuitry. The new check circuit for monitoring of the active signal is also provided for the MD1B circuitry with the identical check circuit other than for the Fast Response A.F Amplifier in the MD1A. The detailed amplifier circuitry of the Metal Detector MD1 is shown in Fig. 16. In the drawings, the active check signals by means of the each Authentication Controller put into the each A.F Amplifier through those new check circuits. A pulse generator circuit and an adjustable signal level circuit of the output compose the check circuitry for the Authentication Controller. As results, the two amplifier, the X-Y Axial and the Z Axial, are modified and are newly made one in indication of enclosed circuitry with chain-lines in Fig. 16.

4.2 Detailed Modification of PN/M System

Basically, the modification of the PN/M Systems was carried out such as the one of the P/M System other than the active output signals to the PN/M sensors and the reconstruction of the PN/M Junction Unit. The PN/M Authentication Controller is installed inside the PN/M Junction Unit in contrast with the P/M Authentication

Controller that is fixed on the top of the P/M Junction Unit as mentioned above.

The all input/output signals between the PN/M system and the PN/M Authentication Controller are isolated electrically by the optical isolators and the relay contacts as well as the P/M system and the P/M Authentication Controller.

4.2.1 Transmission of System Clock from PN/M System to PN/M Authentication Controller

The recorded event data of the PN/M Authentication Controller should be tagged with the time of day and date information to facilitate a comparison between the data of the PN/M Authentication Controller and the data of the PN/M System. Because the Automatic Data Comparison will verify a time discrepancy of between the identical event data caused by both the PN/M Authentication Controller and the PN/M System. Then, both the PN/M Authentication System and the PN/M System have to have the same time of day and date for an event in principle. Therefore, the PN/M System sends the time of day and date information to the P/M Authentication Controller. The clock information consists of Second, Minute, Hour of day, Day of month and Month of year, but the year of calendar. Only last 2 digits of calendar year are set to the PN/M Authentication System through the personal computer for inspector.

The modification of the PN/M System for this purpose was carried out by JAERI. The conceptual diagram of Penetration Monitor is shown in Fig. 2. This conceptual diagram is for the original entire system before the installation of the Authentication System. After the installation of the PN/M Authentication Controller, the block diagram of both the FCA PN/M system and the PN/M Authentication Equipment is shown in Fig. 4. The PN/M Authentication Equipment at the facility consists of the PN/M Authentication Controller, the PN/M DataKey and the Inspector Personal Computer.

The clock signal of the PN/M System is transmitted to the PN/M Authentication Controller via I/O interface circuitry of the PN/M System's CPU and the Multiplex Transmitter Devices (Data Trans) of both the Control Unit and the Junction Unit through the optical fiber transmission cable.

The modification and addition of the system is described hereinafter in down flow manner for the clock signal from the PN/M System's CPU to the PN/M Authentication Controller.

As illustrated in Fig. 26, one Output Interface Board (OUT 2) is newly provided with the I/O Interface Unit of the CPU, and the output signals of the clock from the CPU are sent to the Multiplex Transmitter of the PN/M Control Unit. The total of four modules (Data Trans) are installed at both the Control Unit and the Junction Unit, two Transmitter modules (GDT) at the Control Unit and two Receiver modules (GDL) at the Junction Unit, respectively. Those modules are shown in Fig. 24 and Fig. 25.

The detailed connection of the clock signals from the PN/M CPU I/O Interface to the Multiplex Transmitter modules is shown in Fig. 28 and the detailed connection of those one from the Mltiplex Transmitter modules to the I/O interface circuitry of the PN/M Authentication Controller is shown in Fig. 29 and Fig. 30. The transmittable clock signals are accomplished with Month, Day, Hour, Minute and Second as mentioned above.

4.2.2 Connection of All Sensors' Output Signals Monitored by PN/M Authentication Equipment

The Space Sensors of both the reactor room and the annulus are monitored their activation by the PN/M Authentication Equipment. Therefore, those sensor outputs should be connected to the PN/M Authentication Controller.

As shown in Fig. 4, those outputs are divided into two directional connecting at Terminal Blocks for the Multiplex Transmitter modules of the PN/M JU. At the Terminal Blocks, the one is connected to the inputs of the Multiplex Transmitter modules and the other is wired to the Input/Output Interface Circuitry of the PN/M AC via the Isolated I/O Interface Circuitry that completely isolates the electrical signals of the PN/M System from the one of the PN/M Authentication Controller.

The appearance of parts location on the board of the Isolated I/O Interface Circuitry is shown in Fig. 8 and this circuitry board contained ten couples of Input/Output circuitry is shown in Fig. 9. In this board, the input electrical signals are changed to the dry contact signals as the output signals.

The two Isolated I/O Interface Boards are provided with the new interface circuit shelf inside the new Junction Unit of the PN/M system. As shown in Fig. 24, this PN/M Junction Unit is also provided with the Power Supplies and their switches for the PN/M Authentication Equipment. The circuitry of Power Supplies provided newly is shown in Fig. 27.

The detailed connection of the Space Sensors to the PN/M Authentication Controller through the Isolated I/O Interface Circuitry is shown in Fig. 31 to Fig. 33.

4.2.3 Connection for Active Output Signals of PN/M Authentication Controller to Space Sensors

The records of the PN/M Authentication Equipment provide passive monitoring sensor events and randomly simulated activation events of selected critical sensors. The PN/M Authentication Equipment can monitor individually up to three sensors selected by the IAEA in the PN/M system. Those sensors can also be selected, from any one to all one, for a random active testing, but no other sensors can be chosen for a random active test. Therefore, all simulated output signals of the PN/M AC should be connected with all Space Sensors at both the reactor room and the annulus in principle.

For the active monitoring of all Space Sensors of the PN/M system at both the reactor room and the annulus, the signals for the those sensors' activation by the PN/M Authentication Controller are individually connected together with those sensors outputs at the Terminal Block. Those active signals are also fed to the PN/M Control Unit through the Multiplex Transmitters of both the PN/M Junction Unit and the PN/M Control Unit as shown in Fig. 4.

The detailed connection of all active output signals of the PN/M Authentication Controller to all Space Sensors is shown in Fig. 31 to Fig.33. In the drawings, all simulated sensor signals of the PN/M Authentication Controller are directly connected to the Terminal Block which is joined with all real signals of Space Sensors, but through the Isolated I/O Interface Circuitry. All simulated sensor signals of the PN/M Authentication Controller are composed of the normal closed contacts of their relays for the electrical isolation between the PN/M Authentication Controller and the PN/M system.

4.2.4 Reconstruction of PN/M Junction Unit to Include PN/M Authentication Controller

The IAEA required that the PN/M Authentication Controller is included inside the PN/M Junction Unit to maintain an integrity of the PN/M Authentication Controller under the installation in the place of the FCA annulus. The former Junction Unit of PN/M system could not include some devices for the installation of the PN/M Authentication Equipment. However, the PN/M Junction Unit is necessary to newly contain some devices and circuitry, for example, the PN/M Authentication Controller, the boards of Isolated I/O Interface Circuitry with their shelf unit , AC and DC Power Supplies with their Power Switches and the Terminal Blocks for the wired connection as mentioned above in addition to the original circuitry and devices. As results, the PN/M Junction Unit was rebuilt to the new one for fully compatible with the implementation of the authentication measures.

As shown in Photo 4 and Photo 5, the new PN/M Junction Unit is exactly similar to the old one's appearance other than its dimensions in width, depth and height.

The new PN/M Junction Unit includes completely the devices for the authentication measures and the connection between the PN/M system and the PN/M Authentication Controller as shown in Fig. 24 and Photo 5.

5. Field Test

The development of FCA C/S System was concluded in 1990 after the intensive test for the effectiveness, reliability and efficiency of the system. This conclusion was conditional on the provision of independent IAEA authentication equipment and on some improvements as specified in the Final Report "Field Trial – Fast Critical Assembly (FCA) Containment and Surveillance (C/S) System" [8]. In accordance with this conclusion, the Authentication Equipment was developed under the IAEA responsibility with the financial and technical support from JAERI and with the extensive collaboration of the SNL. Therefore, the Authentication Equipment developed by the IAEA should not affect the performances of the effectiveness, reliability and efficiency established.

In this context, the first priority of the field test should be devoted to verify the proper function of the authentication equipment installed and to establish its reliability.

The field test of the authentication system was mostly divided into two stages, the first field test only for the Authentication Equipment, mainly the Authentication Controller, and the second field test for the Authentication Equipment with the Automatic Data Comparator at the initial stage. As a result, the second field test was carried out as two phase field tests of "Short Term and Extended Field Test of FCA Authentication Controllers with Data Comparator" and "Extended Second Field Test".

5.1 First Field Test

5.1.1 Pre-Installation Meeting

In August 1991, a meeting on pre-installation of the FCA C/S system authentication equipment was held at FCA with participants from the IAEA, JAERI, SNL and Shimadzu Co. Ltd.. The pre-installation issues were discussed and decided by all participants as follows:

(1) The field test procedure for both the FCA C/S equipment and the Authentication Equipment was discussed to establish that procedure and to assure that the Authentication Equipment does not interfere with the C/S equipment operation.

(2) The capability of walk-through test of the P/M and the PN/M systems was examined for checking of the proper operation of the Authentication

Equipment and a more refined field test could be developed prior to installation.

(3) The shipment of the Authentication Equipment to the FCA facility.

(4) The mechanical installation in detail.

(5) Available opportunities for the equipment installation.

(6) The IAEA provision for an IBM PC compatible laptop computer, printer and cables including RS232 cable prior to installation.

(7) JAERI provided a graph of MD response as a function of time elapsed.

(8) A set of drawings describing the Authentication Equipment was left with JAERI by SNL.

"Plan for Field Test of the FCA C/S System with Authentication Controllers" was submitted by S.Yim (SH-OA1,SGDE,IAEA) to T.Someya (Inspector General, JNSB) in November 1991. But the plan was revised as "Plan for Field Test of the FCA C/S System Authentication Controllers" by the proposal of the JAERI to test only the Authentication Controller except the FCA C/S System as mentioned reason above.

The plan for field test of the FCA C/S system Authentication Controller mentioned the following issues as "Purpose of field test", "Criteria for acceptance", "Time schedule", "Responsibilities" and "Activities to be carried out".

Purpose of field test

(1) To find out whether the authentication component of the C/S system functions as intended.

(2) To propose modifications and/or improvements to the Authentication Controllers as applicable.

(3) To find out whether drafted inspection procedures relating to the operation of the C/S system are appropriate.

Criteria for acceptance

In the evaluation of the results of the field tests, the following factors should be considered :

(1) Reliability.

Do the Authentication Controllers respond properly to their self tests and to manually triggered tests ?

(2) False alarm rate.

(3) Self-annunciation of failure.

(4) Efficiency.

Can the Authentication Controllers be operated with the C/S system and its results interpreted by the inspectors with reasonable effort ?

(5) Compatibility.

Do the Authentication Controllers operate without adversely effecting the overall function of the C/S system ?

Time schedule

The initial training on the operation of the Authentication Controllers.

The opportunity for familiarization and training.

Starting and finishing periods of the field test in connection with the routine inspections.

The C/S system shall be serviced monthly in connection with routine safeguards inspections.

The initial and monthly review of results from both the FCA C/S system and the Authentication Controllers.

Responsibilities

For conducting and evaluating the field test, SGOA and SGDE share jointly.

SGDE has responsible for technical coordination, evaluation of results and production of the field test report, and possible negotiation with JNSB.

Activities to be carried out by IAEA staff

(1) At HQ :

Training of inspectors on the simulator.

Collection and analysis of tapes and printouts.

Changes or additions to procedures and documentation.

Formulation of recommendations to the JNSB and JAERI or SNL on equipment modifications and improvements.

Production of Test Report.

(2) At TRO :

Programming of DataKey.

Preparation of laptop computer, data diskettes, DataKey, video tapes, seals, wire and working papers.

(3) At FCA :

Servicing of and collection of data from the C/S system according to procedure checklist.

Initial evaluation of collected data.

Programming (re-programming) of the Authentication Controller.

The servicing procedure at FCA includes the P/M and the PN/M authentication tests as follows :

(1) P/M Authentication Tests
Manual metal detection test.
Manual sensor trigger.
Sensor monitoring.
Metal detector test.
AC power cut.

(2) PN/M Authentication Tests
Manual sensor triggering.
Sensor monitoring.
Active sensor test.
AC power cut.

5.1.2 Installation of Authentication Controllers and Preliminary Test

The P/M and the PN/M Authentication Controllers were installed tentatively. A preliminary test was carried out by participating with the IAEA, JNSB, SNL, JAERI and Shimazdu Co. Ltd. at FCA on November 20 to 26, 1991. Demonstrations of the authentication system software and training in the system operation were also carried out at the same time.

At this time, there was some confusion for the Input/Output Interface between the FCA C/S System and the Authentication Controller. This problem was resolved by modifying the embedded firmware and hardware. On the end of Friday, both the Authentication Controllers were left in data acquisition for the weekend. After that, a problem was found out with a DataKey procedure and was corrected with a modification to the firmware.

The performance test of the Authentication Equipment including a one-hour battery test were done prior to start the first field test. A teething trouble of the system was found out and corrected.

For the field test, the P/M and the PN/M Authentication Controllers were operated in acquisition and both the Junction Units were sealed up, and the P/M Authentication Controller enclosure was also sealed while it was located outside the P/M Junction Unit.

The program requirements of adding an automatic comparison capability to the existing authentication system were discussed in connection with its fund among the parties during this period. It was mentioned that the automatic comparison of data greatly eased the inspector's task of comparing the data recorded by the two systems and reduce the opportunities for human error.

5.1.3 First Field Test and its Results

The first field test was started after the successful installation of the P/M and the PN/M Authentication Controllers at the FCA facility on November 26, 1991. The test in accordance with "Plan for Field Test of the FCA C/S System Authentication Controllers" was performed in four periods, November 26 to December 16, December 16 in 1991 to January 27 in 1992, January 27 to February 17 and February 17 to March 16 when the test was finished. But the first period of November 26 to December 16 was considered as a pre-test period.

The Authentication Controllers were serviced at approximately one month intervals in conjunction with monthly routine inspections during the field test.

Criteria for Acceptance of Authentication System

In reference to the test report "Field Test Fast Critical Assembly (FCA) Authentication Equipment", an acceptance criteria of the authentication system was described in detail as follows:

In evaluating the results of the field test the following factors were taken into consideration :

(1) Reliability :

(a) Are all activation of sensors properly recorded in the Authentication Controllers files (for both P/M and PN/M) ?

(b) The system should work unattended for periods longer than one month (24 hours a day) without failure of the electric system. Does the system fulfill that criteria ?

(c) Do the Authentication Controllers respond properly to self-tests and manually triggered tests ?

(2) False alarm rate :

Are events which are neither real nor triggered test events recorded by the

Authentication Controllers ?
Do the Authentication Controller fail and without record of the error ?

(3) Efficiency :
Can the Authentication Controllers be operated with the C/S system and the results interpreted by the inspectors with minimum additional effort ?

(4) Compatibility :
Do the Authentication Controllers operate without adverse effect on the overall function of the FCA C/S system.

(5) User friendliness :
Is the system easy to operate ? Are the menus and screens of all parts of the system self explaining and is the inspector guided through the various menus to simplify inspection work ? Are activities which can have large influence on system operation (like Quit etc.) demanding further confirmation from the inspector in order to minimize the possibility of premature system shutdown ?

Summaries of the field test results

The field test showed that :

(1) Comparison of events in both data files is extremely difficult.

(2) Some events were spotted where the system did not respond as expected.

(3) After discussing the occurrence of these events with the developer, changes in the software were undertaken in order to achieve a satisfactory operation of the whole C/S system. The corrective actions are listed.

(4) Operating the Authentication Controller is reasonably easy by means of menu displays and guiding instructions on the screen.

(5) Programming of the parameters to be monitored or activated by the Authentication Controllers is easy using the DataKey programming module. Since the parameters cannot be retrieved from a programmed DataKey, the parameters should be double-checked upon input.

(6) One important conclusion is that an automatic data comparator must be included in the system. The amount of time required for the manual comparison of the data records is very large and imposes too much load on the inspector.

Judging the performance of the Authentication Controller according to the criteria for acceptance

(1) Reliability :
Events were spotted where the system did not respond as expected.
No hardware problems were detected during the whole period of the field test.

(2) False alarm rate :
No false alarms were recorded by the Authentication Controllers.

(3) Efficiency :
Manual comparison of data files was very inefficient. The increase of workload imposed upon the inspector was unacceptable.

(4) Compatibility :
No influence on the functioning of the C/S system was detected. The Authentication Controllers were not effecting the performance of the C/S system.

(5) User friendliness :
Operating the Authentication Controllers and DataKey programming equipment is reasonably simple. The inspector is guided during operating the equipment by means of menus and screen instructions. In one case it was possible to shut-off accidentally the system without getting a message that data transfer to the diskette was not finished. This effect was already corrected by the developer.

5.2 Second Field Test

At the beginning of the field test, the IAEA proposed a continuos six months running period, at least or more than if applicable. In the nature of FCA, it was not applied for the field trial and therefore both parties agreed with a continual six months period with an unattended monthly period (24 hours per day, at least 30 days per month) in conjunction with a monthly inspection for the field test. Consequently, the second field test was carried out from the end of November 1992 to April 1993.

5.2.1 Test Plan for Short Term and Extended (Follow Up) Field Test

The draft test plan of "Short Term and Extended (Follow Up) Field Test of FCA Authentication Controllers with Data Comparator" for the field test was submitted to JNSB by the IAEA prior to commence the installation and test of both the modified Authentication Controllers and the Automatic Data Comparator. The test plan was revised later and was agreed with both parties, the IAEA and Japan side.

This field test plan defines following extensive items such as "The First Field Test Plan".

A complete test reflecting all changes made in the Authentication Controllers software and the newly developed the Automatic Data Comparator was envisaged to begin at the end of November in 1992.

Purpose of field test

The main purpose of the field test is to test the Authentication Controllers and the Automatic Data Comparator as follows:

(1) Test the function of the Authentication Controllers.

(2) Test the function of the Automatic Data Comparator.

(3) Propose modifications and/or improvements to the Automatic Data Comparator (or Authentication Controllers) to improve their functionality and efficiency as applicable.

(4) To find out whether draft inspection procedures relating to the operation of the complete system (C/S, Authentication Controllers, DataKey program and Automatic Data Comparator) are appropriate.

(5) Discuss all problems, clarify all unclear points, evaluate test results and re-test the system on site (if necessary) in order to complete testing as soon as possible.

Criteria for acceptance

(1) Functionality.

(2) Reliability.
Inspections are presently carried out monthly.
The authentication system should work unattended 24 hours per day for at least 30 days.

Do the Authentication Controllers respond properly to self-tests and to manually triggered events ?

Can the authentication system, in case of failure, record some messages indicating the occurrence of a failure (error messages) ?

(3) False alarm rate.

(4) Efficiency.

Does the authentication system increase the efficiency of inspections ?

The total effort for servicing the C/S system and evaluating collected data should be taken into account when considering this matter.

(5) User friendliness.

Time schedule

Check up and initial testing was carried out by the developer, SNL, in conjunction with the demonstration of the new authentication and the data comparator software.

The follow-up test was divided into two phases :

Phase 1 :

Testing of complete authentication system in presence of all parties involved was carried out.

In this part of the test the Authentication Controllers would be re-tested to find out if all problem discovered in the last field test were resolved.

All recorded events were evaluated manually at that time.

Problems, questions, unclear effect, recommendations and suggestions for improvements were discussed during the evaluation of that phase of the test on site.

The results of the Automatic Data Comparator were compared to the results of the manual comparison.

Phase 2 :

After completion of the first phase of the test a decision was taken whether the C/S system with all its components was mature for the extended (phase 2) of the field test at its current status, and also whether further modifications were needed before such test.

No modification in the accepted C/S system was done.

Phase 2 of the field test was planed for 2 months.

Results of the comparison should be manually checked against the printouts of the C/S and the authentication systems.

The parameters of the authentication system should be changed from one inspection to the other.

In both parts of the test, the video surveillance tapes must be reviewed in order to confirm all activities recorded in the C/S system. This gave a confirmation of proper operation of the surveillance system.

Responsibility

It was defined individual duties of all parties such as the previous test.

Actions

(1) Developer (SNL)

The SNL staff (Mr. K.Ystesund) demonstrates the new software of the Authentication Controllers and the Automatic Data Comparator.

System manuals, technical documentation and operating manuals (at least in draft form) must be available for the field test.

A complete set of the authentication and the data comparator software must be given to the IAEA through JAERI.

Initial training to IAEA inspectors and SGDE staff was given by the SNL in conjunction with phase one of the field test.

Undertake any necessary modifications during phase one or two of the field tests and support SGOA and SGDE in evaluating results (via FAX, phone - as necessary).

(2) IAEA staff – at HQ

Training of inspectors on the simulator prior to their taking part in field test servicing.

Collection and analysis of tapes (video) and printouts.

Recommendations and implementations of changes or additions to procedures and documentation.

Formulating recommendations to JNSB and JAERI or SNL on equipment modifications and improvements.

Carry out evaluation of field test results on data sent from TRO to the IAEA HQ's.

Production of the test report.

(3) IAEA staff – at TRO

Programming of DataKey.

Preparation of a laptop computer, a communication cable, data diskettes, DataKeys, video tapes, seals, wire and working papers.

(4) IAEA staff – at FCA

Attending training of system given by SNL personnel.

Operating the Authentication Controllers and the Automatic Data Comparator.

Taking part in evaluation team of field test results.

Attend meetings for discussing problems, questions and suggestions of all subjects related to the field test.

Servicing of and collecting of the data for the C/S system according to procedure checklist.

During phase two of the field test, collect the data, run comparison on the Automatic Data Comparator, evaluate the data, review surveillance video tapes and send data evaluation results to HQ for further evaluation.

Program the DataKey for the Authentication Controllers if necessary.

(5) JAERI personnel

All of the decisions of modifications or improvements, made by the SNL, of the authentication system are subject to JAERI approval.

Test plan

Basically all parameters and functions of the complete system should be checked to be sure that all changes after the last field test had the proper effect.

Initial tests should be carried out by SNL staff to ensure proper operation of the data comparator system. After completing this, an introductory training should be held at FCA on how to operate the Authentication Controllers and the Automatic Data Comparator.

DataKeys must be programmed and test parameters must be loaded into the system, and the system can begin monitoring the C/S system.

The following steps were included in phase one of the test :

(1) Check all screens and menus for “user-friendliness”.

(2) Data to be programmed into the DataKey :

For the P/M system : sensors SB4, SS6, EMD.

MD test 50 % of occupancy.
1 hrs. time interval.

For the PN/M system : sensors S1O,S2O,S1I – passively monitored.
S1O,S2O,S1I – actively monitored.
Time interval – 1 hrs..

(3) Test of sensors

For the P/M system :

Test of Metal Detector : going through MD with test coupon in both directions.
Entering MD and returning before reaching zone 3 (MD exit towards reactor).
Walk through MD very slowly with test coupon (DIR B) causing "time-over".
Two persons – one at entry, the other at exit of MD causing "multiple occupancy".

Test of sensors : go from SB1 to SB6 and in opposite direction.
Pass SB1,SB2 and return without passing SB3.
Pass SB3,SB4 and return without passing SB6.
Approach SS6 and other Space –Sensors watch their activation.

For the PN/M system :

Test of sensors : approach sensors and watch their activation.

During testing, the P/M and the PN/M systems switched AC Power off for at least 20 minutes, activated all selected sensors and switched AC Power on again.

Record all activation and compare those events with the events of the printout of the P/M and the PN/M Authentication Controllers. All events must be recorded on the printouts.

(4) After finishing phase one test :

Download the data files from the C/S system, the P/M and the PN/M Authentication Controllers into the data comparator computer.

Run the data comparator software.

Measure and record the time required for completion of the comparison process.

Analyze the results of data comparison test.

Verify results of the Automatic Data Comparor by manually comparing the data files (compare the time required for manual and automatic data comparison).

(5) Review all surveillance tapes to confirm events recorded in data files (are all cameras working through the whole test period ?).

(6) Summarize results in report and get approval of results by ALL participants.

The second phase of the field test was planed after SUCCESSFUL completion of the first phase of the field test.

In that period the authentication system should run under normal operating conditions with parameters for the Authentication Controllers changed from an inspection to next inspection in the TRO.

5.2.2 Short Term and Extended Field Test

During the week of November 30, 1992, JNSB, the IAEA, SNL and JAERI personnel participated the meeting and carried out the preliminary test prior to start the short term (Phase 1) and consecutive extended (Phase 2) field test at the FCA facility of JAERI. All parties participated and also discussed the field test plan for the short term and extended (follow up) field test and agreed it. At the meeting Manuals for the authentication system and the Automatic Data Comparator were provided by SNL. But the development of this software and documentation by SNL was founded by JAERI.

At the short term test the Authentication Controller had irregularities regarding the time label of its records. Consequently, the extended field test started late for one month. The extended field test was carried out for three months period from January to April 1993.

1) The short term field test

The work plan and objectives were ,at first, confirmed by the participants.

The updated EPROMs were installed in the P/M and the PN/M Authentication Controllers and also the integrated circuits (ICs) of the Authentication Controllers were replaced. The updated Onsite program of the Authentication Equipment was provided and demonstrated by SNL.

From November 30 (Mon.) to December 4 (Fri.), the Authentication Controllers with the C/S system were repeatedly conducted a short test operation to verify the functions of the Authentication Equipment. After each test the controllers were stopped and the data was collected for comparisons to the C/S system. The comparison was made with the Automatic Data Comparator and a manual comparison of event records was executed to verify the operation of the Automatic Data Comparator.

During 5 days the Authentication Equipment and the Automatic Data Comparator were modified as follows:

For the Authentication Equipment,

a replacement of EPROM in the P/M Authentication Controller to accommodate the holding time for the Metal Detector self test function.

For the Automatic Data Comparator,

the following parameters were programmed.

(a) Time window for the beam sensors.

(b) Time window for all other sensors.

(c) Event bridge time of the metal detector.

At the request of the IAEA,

(a) Screens are added before ending acquisition to verify that the inspector wants to take this action for stopping.

(b) The comparator uses the START-ACQ (acquisition) time rather than the first event time to begin comparisons.

Conclusion

(1) The updated Onsite software was approved by the participants and found to be user friendly and to perform satisfactory.

(2) The automatic comparator performance was verified by manual comparisons. The Automatic Data Comparator significantly reduces the time and effort for the data comparison.

(3) It was agreed that a test of three months will commence immediately and, if necessary, a second test will follow.

(4) JAERI requested that SNL provides a report of the authentication activities including a summary of all work founded by JAERI.

The FCA operator planed an AC power outage for their annual maintenance during the weekend of December 4 and 5 in 1992, then it was decided that a short term test of the authentication system with the FCA C/S system carry out at the time, from 3 to 7 December, in order to check how the system cope with that condition.

Under the participation of both JNSB and IAEA inspector and some JAERI personnel on December 7, the Authentication Controller and the FCA C/S system was tested, for example the Walkthrough Test, by the IAEA inspector prior to stop the systems for the system evaluation of the Authentication Controllers under the condition of power outage.

While the systems was stopped and collected the data, the irregularities regarding the time label of the Authentication Controller record were found. Furthermore both the P/M and the PN/M Authentication Controllers could not be started up for the next new acquisition period. It was determined the cause of the problem that it was not primarily compatible with the start-up sequence of the FCA C/S system following the facility power outage.

2) The extended field test

The revised Onsite software was installed into the Authentication Equipment prior to commence the three months period field test. The field test data was checked monthly by participating three parties, JNSB, the IAEA and JAERI, and the test was continued to evaluate the compared data from January to April 1993.

The inconvenient situation during the first two months of the field test was the extensive use of the Equipment/Emergency Door (EMD) for the criticality experiment by the frequent changing configuration of the assembly core. Under this condition, the whole Metal Detector was bypassed by using the EMD. As a result the Authentication Controller had a large number of wrong sequence as "INCORRECT SB4,5,6 SEQ" in activating the beam sensors of the P/M system. On the one hand, the system detected all of the EMD openings.

The many events with an improper time stamping of the comparator printout were caused by the comparator software which was improperly configured to adjust for the summer time (daylight saving time) when the events were reformatted for printing.

For the last month of the field test the P/M system was used in the routine way of operation. Therefore, in that period the number of unmatched events was drastically reduced.

The Interim Report of the FCA Authentication Equipment and the Automatic Data Comparator described the evaluation results. The main conclusions and the recommendations were as follows :

The results of the evaluation of the last field test

1) For the PN/M

- The Authentication Controllers had not the time stamp through the FCA C/S system in case of the power outage of the facility.
- Only few events of the S4I sensor were left incomparable because of the out of the time window set for the comparison.
- The number of unmatched events left after running the comparator software was drastically reduced so that the inspector was able to compare those unmatched events with reasonable effort.

2) For the P/M

- The beam sensor SB6 was a malfunction.
- All unmatched events of the beam sensor SB6 were outside the time window.
- Metal Detector events for the ten volts output (MD10A and MD10B) did not always respond when the self test circuit of the MD1 was actuated.
- The issue of calibration and false alarms must be evaluated again and a procedure established to avoid unnecessary difficulties.

The main conclusions

1) Power failures occurred because of problems with the Uninterruptible Power Supply (UPS) used.
2) The timely behavior of the various sensor was not constant.
3) The system was not used in the way it was designed for (the EMD was opened most of the time, multiple occupancy).
4) It seems as if the calibrating of the Metal Detector coils is causing false alarms (% Test).

The recommendations for the next field test which is anticipated to begin in 1993

1) The Equipment/Emergency Door (EMD) is proposed to be sealed to assure that the system is used according to the agreed procedure.
2) The percentage test should be programmed in the DataKey to 0 %. The events of Metal Detector "% test" failed are expected to be eliminated in that case.
3) Evaluation of the results after running the data comparator software, should be done on the site at the end of the inspection. It might be necessary to add an additional work day for that purpose.
4) It should be noted that an improved Uninterruptible Power Supply (UPS) is going to be used so that power problems will hopefully be eliminated.

The use of the Automatic Data Comparator reduces the number of unmatched events significantly and there is no doubt that without it the system could not be used in practical sense.

5.2.3 Extended Second Field Test

In accordance with the recommendations for the next field test on the Interim Report of the FCA Authentication Equipment and the Automatic Data Comparator, two Uninterruptible Power Supplies (UPS) of the P/M and the PN/M systems were replaced with new improved ones in June, 1993. In August, an SNL personnel exchanged two EPROMs of both the P/M and the PN/M Authentication Controllers to cope with an issue of 2000 calendar year.

A pretest of one week long for the authentication system was carried out with three parties attended in February 1994, prior to commence three periods of the extended second field test from February to May 1994. After the one week operation, a data comparison using the Automatic Data Comparator was executed between the Authentication Controllers' data and the FCA C/S system's data. There was no unmatched data in the P/M system, and there were only two unmatched events in the PN/M system.

One week later after the completion of the pretest, three sub-periods of the field test were commenced in February 1994, and continued by May, 1994.

The purposes of the field test were achieved as follows:

- Activation on a random basis of selected the P/M and the PN/M sensors.
- Passive monitoring of selected the P/M and the PN/M sensors.

The purposes of the field test were defined as follows:

- To find out whether the authentication component of the C/S system functions as intended and that the selected parameters for monitoring are correctly monitored by the Authentication Controllers.
- Check functionality of data comparator and observe the amount of time required to complete evaluation of comparator printouts.
- To propose modifications for improvements to the Authentication Controllers and the Automatic Data Comparator as applicable.

This field test was carried out in accordance with the detailed test plan that was prepared in January 1993 and was also mentioned above section 5.2.1.

The IAEA seals were applied to the penetrations of the reactor room (hatches of fuel transferring and the emergency hatch), the Equipment/Emergency Door of the

P/M system and the Control Unit's doors of both the P/M and the PN/M systems through the entire field test. The IAEA seals were also applied to the P/M and the PN/M Authentication Controllers ,the P/M Junction Unit doors and the PN/M Junction Unit doors.

Test results of the field test

After executing the data comparison, all unmatched events for all three periods of the extended second field test were decided as follows:

1st period : Feb. to March, 94	zero event in P/M,	one event in PN/M.
2nd period : Mar. to April, 94	12 events in P/M,	zero event in PN/M.
3rd period : Apr. to May, 94	18 events in P/M,	zero event in PN/M.

It was indicated that the system was used in the way it was designed to operate through this extended second field test.

Detailed Unmatched Events

1) PN/M data comparison

There was only one unmatched event through the three sub-periods of the field test. This unmatched event was happened on the S1O infrared motion sensor at the starting time of the PN/M Authentication Controller by an inspector. This motion detected by the system was recorded as the unmatched event. Therefore, the inspector is required to stay there and not to move from the time its Authentication Controller initiated the sensor test until the computer's display for the inspector indicates that the self test is completed.

2) P/M data comparison

The unmatched events of P/M data comparison are assorted below.

Unmatched Events	1st Period	2nd Period	3rd Period	Total
MD Test Failed	0	2	13	15
Incorrect SB4, 5, 6 SEQ	0	4	1	5
Unmatched Events of SB4	0	5	0	5
Unmatched Events of SB3	0	1	0	1
Unmatched Events of SB1	0	0	4	4
Total Events	0	12	18	**30**

MD Test Failed

The MD Test Failed message indicates that the metal detector failed to return the expected results when a metal detector test was initiated. The 15 total events of MD Test Failed were caused by tests based on a percentage of occupation (PERCENT) and a random time (TIME), then PERCENT was 9 events and TIME was 6 events.

The metal detector output consists of four outputs (MD1A5, MD1A10, MD1B5 and MD1B10, i.e., two 5 volts and two 10 volts outputs) and the authentication system monitors that all four metal detector outputs respond when a metal detector test is initiated. The tests failed because the ten volts output of the MD1A10 in the Metal Detector did not respond when the self test circuitry of the MD1 Metal Detector was actuated. But the ten volts output of the MD1B10 was always respond correctly.

The metal detection circuitry of the MD1 Metal Detector is designed to intend a detection of one fuel plate (size, 2 inches x 2 inches x 1/16 inches) as a 5 volts output (MD1A5 and/or MD1B5) in principle. Therefore, 10 volts output (MD1A10 and/or MD1B10) means to detect a relatively large and/or massive metal subject rather than the fuel plate. Accordingly, the MD Test Failed for "10 volts output" is not a fatal failure in that test, but it is essential that 5 volts output is always respond correctly when a metal detector test is initiated.

The MD1 Metal Detector is very sensitive device so that temperature variations may cause to affect the response of its amplifiers.

Incorrect SB4, 5, 6 SEQ

Unmatched events during the 2nd and 3rd period field test periods were recorded as "Incorrect SB4, 5, 6 SEQ". These unmatched events are generated on two conditions that are analyzed by the Authentication Controller. These conditions are as follows:

1) The activation sequence of the sensors is other than both SB4 – SB5 – SB6 in turn (Direction – A, coming into the reactor room) and SB6 – SB5 – SB4 in turn (Direction – B, going out of the reactor room).
2) This sequence must be completed within 10 seconds.

Four Incorrect SB SEQ events at the 2nd period field test were caused by the first reason above. A log of Daily Events of the P/M system indicated clearly that some personnel of FCA staff went out of the reactor room through the Portal Monitor accompanying with the Time Over (Zone 3) at that time.

One Incorrect SB SEQ event at the 3rd period field test was caused by the second reason above. A log of Daily Event of the P/M system indicated clearly that some person went back from the place inside the P/M system with an indication of "B and $". Incidentally, this indicator ($) means that a person will back out of the inside of the MD monitor passage to its entrance.

If this unmatched event would be recorded by a data comparison, inspectors will understand easily this situation in a short time by reference to a Daily Event Log of the P/M system.

Unmatched Events of SB4

Events out of 5 unmatched SB4 events were recorded on April 1 at the 2nd period field test. These unmatched events were caused by a time difference in the sensor response when the SB4 were triggered. A nominal response time window for the SB sensors is within the ±8 seconds, and also the Authentication Controller has the same time window in its software. But the real response time window of the FCA C/S system is within ±9 seconds, then its time window should be concerned for a digitized value which has the ±1 difference in the nature of digitizing. Therefore, the time window for the SB sensors on the Authentication Controller should be spread to 9 seconds window from 8 seconds window. If this time window is accommodated to the real condition, the unmatched events by the time difference will not be observed.

Unmatched events of SB3 and SB4

One unmatched SB3 event and two unmatched SB4 events were consecutively recorded by only one second difference each other on April 6 at the 2nd period field test. These unmatched events were caused by the same condition mentioned above.

The Time-Over in Zone 3 accompanied with a person passed were caused by another different reason. The person truly stayed at Zone 3 more than 10 seconds. Consequently, the Daily Event Log of the FCA C/S system indicated correctly the Time-Over in Zone 3 while that person passed there.

Unmatched events of SB1

Unmatched SB1 events were recorded during the 3rd period field test. Two unmatched evens of SB1 were indicated on May 10, and later two unmatched SB1 events were indicated on May 23. When these events occurred, FCA C/S

Log indicated both a Time-Over in Zone 1 and a Multi-Occupancy. These events mean that two persons consecutively entered into Zone 1 of the Portal Monitor at the same traffic, and one person stayed more than 10 seconds at Zone 1.

The time difference at the beginning of the event between the FCA C/S system and the P/M Authentication Controller was indicated 10 seconds. Consequently, the time window for the SB sensors seem to require for changing from 9 seconds to 10 seconds.

5.2.4 Conclusions and Recommendations

The final field test report of the Authentication Systems and the Automatic Data Comparator issued by the Department of Safeguards of IAEA describes “Conclusions and Recommendations” as follows:

Conclusions

It was found that the use of the Automatic Data Comparator extensively reduces the amount of effort required from the inspector while performing his inspection activities.

The Authentication Controllers are operating the way they were designed to and the FCA C/S system performance – operator designed – is being well monitored by the Authentication Controllers.

Judging the performance of the Authentication Controllers and the Automatic Data Comparator

According to the criteria for acceptance, the IAEA wishes to make the following conclusive remarks:

a) Reliability:
- No hardware problems were detected during the whole period of the field test.
- Metal detector calibration needs to be looked at.
  Not all coils were activated during initializing self-tests (MD1A10).

b) False alarm rate:
- False alarms were only detected in conjunction with the metal detector self test.

c) Efficiency:
   - The use of the Automatic Data Comparator significantly improved the efficiency of the system.

d) Compatibility:
   - No influence on the function of the FCA C/S system was detected. The Authentication Controllers were not effecting the performance of the FCA C/S system.

e) User-friendliness:
   - Operating the Authentication Controllers, the DataKey program and the Automatic Data Comparator was reasonably straightforward. The inspector was guided during operating the equipment by means of menus and screen instructions.

Recommendations

Recommending the acceptance of the system for routine use as an approved safeguards system for the FCA facility will depend on the results of practical experience gained.

6. Development Progress on Authentication System of FCA C/S System

1. July,1988 — Authentication proposal letter from H.Kurihara (IAEA, SGDE) to H.Tani (JNSB).

2. September, 1988 — Letter for JASPAS/POTAS collaboration on the authentication development for FCA C/S System, J.Jennekens (IAEA, DDG-SG) to K.Takagi (JNSB).

3. October, 1988 — Specification of the Authentication Equipment, L.Watkins (IAEA, SGDE).

4. May, 1989 — Letter on authentication,
K.Naito (IAEA, SGDE) to K.Takagi (JNSB).
August, 1989 — K.Takagi (JNSB) to K.Naito (IAEA,SGDE).

5. February, 1990 — Letter for an approval of the system on condition that an independent IAEA Authentication Equipment is provided, J.Jennekens (IAEA, DDG-SG) to J.Shibata (JNSB).

6. May, 1990 — The authentication design review meeting at SNL,
IAEA: E.Yellin(SGDE), J.Janov, S.Beach(SGOA)
SNL: D.Mangan, C.Sonnier, K.Ystesund. etc.
JAERI: T.Mukaiyama.

7. June,1991 — Both the P/M and the PN/M systems were modified for the authentication application.

8. August, 1991 — Meeting on the pre-installation of the FCA C/S system Authentication Equipment at the FCA, Syde-Azmi(SGOA), K.Ystesund(SNL), T.Mukaiyama, H.Ogawa(JAERI), K.Tamura, J.Yoshida(Shimadzu).

9. November, 1991 — Plan for Field Test of the FCA C/S System Authentication Controllers, S.Yim (SH-OA1,IAEA) to T.Someya (Inspector General, JNSB).

10. November, 1991 At first, the Authentication Controller was installed tentatively for a preliminary test at FCA.
The Authentication Equipment was installed completely and tested for the field test.

11. November, 1991 to March, 1992 1st field test of the Authentication Equipment.

12. November, 1992 Draft Test Plan,
Short term and extended (follow up) field test of FCA Authentication Controllers with the Automatic Data Comparator,
M.Goldfarb (SGDE), R.Ekarv (SGOA).

13. December, 1992 The Automatic Data Comparator software was delivered to FCA from SNL, and a portion of the Authentication Controller firmware was improved by resulting from the 1st field test.

14. January, 1993 Test Report,
Field Test Fast Critical Assembly (FCA) Authentication Equipment,
M.Goldfarb (SGDE), R.Ekarv, K.Rzymkowski (SGOA).

15. December, 1992 to April, 1993 Short term and extended field test (1st Phase) of both the Authentication Equipment and the Automatic Data Comparator.

16. June, 1993 Two Uninterruptible Power Supplies (UPS) of both the P/M and the PN/M systems were replaced with new improved UPS.

17. August, 1993 To cope with a problem of 2000 calendar year, two EEPROMs of the P/M and the PN/M Authentication Controller were replaced with new ones.

18. February, 1994 Interim report of the Fast Critical Assembly (FCA)

Authentication Equipment and Automatic Data Comparator field test (Dec. 92 – April 93), M.Goldfarb (SGDE), R.Ekarv, K.Rzymkowski (SGOA).

19. February, 1994 Pre-Test of both the Authentication Equipment and the C/S system.

20. February, 1994 to May, 1995 The extended 2nd field test (2nd Phase) of both the Authentication Equipment and the Automatic Data Comparator.

21. May, 1995 The final field test report of the authentication system and the Automatic Data Comparator (Feb. – May 1994), M.Goldfarb (SGDE), K.Rzymkowski, R.Ekarv (SGOA).

22. September, 1996 This project was completed.
The entire system including the authentication system is used for routine inspections.

Acknowledgments

The development of the portal and penetration monitors for FCA was initiated by the suggestion of H.Kuroi of JAERI, who is presently at the Japan Nuclear Fuel Ltd. The authors gratefully acknowledge his valuable suggestion and encouragement for the development of authentication system of FCA. Thanks are gratefully extended to D.Rundquist, L.Watkins, E.Yellin and M.Goldfarb of the IAEA, who were the IAEA task officers for this project. The authors also thanks to K.Ikawa of JAERI for his support and encouragement.

The authentication system for the P/M and PN/M systems of the FCA was developed jointly with the Sandia National Laboratories (SNL) through the Department of Energy of USA (USDOE). The authors gratefully acknowledge K.Ystesund and his staff for their efforts.

The authors gratefully thank the IAEA inspectors and the JNSB inspectors for their help and support during field tests, especially, R.Ekarv, K.Rzmkowski, S.Beach and Syed-Azmi.

The authors thank the FCA staff for their help and support for the development and for the field tests, especially, K.Kurosawa and H.Sodeyama for their support during the field tests. Thanks are also to members of Safeguards Technology Laboratory, which is presently Nuclear Materials Management Technology Laboratory since April 1997, of JAERI for their valuable support.

This work was performed jointly under the framework of the Japan Support Programme for Agency Safeguards (JASPAS) and the U.S. Program of Technical Assistance to IAEA Safeguards (POTAS), and also under the research agreement between JAERI and USDOE.

References

(1) T.MUKAIYAMA, H.OGAWA, Y.YOKOTA, H.KUROI, P.VODRAZKA, A.MATOLCSY, "Development of portal and penetration monitoring system of the fast critical assembly FCA for the international safeguards", Proc.6th ESARDA symposium (1984), p111.

(2) T.MUKAIYAMA, Y.YOKOTA, H.OGAWA, H.KUROI, "Progress in development of containment and surveillance system at JAERI", INMM 28th Annual Meeting Proceedings, Volume XVI, p383-388, Newport Beach, Calif., July 12-15, 1987.

(3) T.SHEA, D.E.RUNDQUIST, K.GAERTNER, E.YELLIN, "Use of operator-provided, installed C/S equipment in IAEA safeguards", INMM 28th Annual Meeting Proceedings, Volume XVI, p389-399, Newport Beach, Calf., July 12-15, 1987.

(4) L.WATKINS, D.E.RUNDQUIST, "Authentication of an operator-provided Containment and Surveillance (C&S) system", INMM 28th Annual Meeting Proceedings, Volume XVI, p585-591, Newport Beach, Calif., July 12-15, 1987.

(5) K.J.YSTESUND, A.PERLINSKI, K.YOUNG, M.L.GARCIA, E.YELLIN, J.JANOV, D.E.RUNDQUIST, T.MUKAIYAMA, M.GAILLOUR, "Authentication system for at the Fast Critical Assembly (FCA)", INMM 31st Annual Meeting Proceedings, Volume XIX, p683-687, Los Angels, Calif., July 15-18, 1990.

(6) K.J.YSTESUND, M.J.BAUMANN, K.W.INSCH, A.W.PERLINSKI, A.E.DAKOFSKY, T.MUKAIYAMA, "Authentication system for the JAERI fast critical facility advanced containment and surveillance system", INMM 33rd Annual Meeting Proceedings, Volume XXI, p659-662, Orlando, Fla., July 19-22, 1992.

(7) H.OGAWA, Y.YOKOTA, T.MUKAIYAMA, "FCA Containment and Surveillance (C/S) System", JAERI-Research 94-026 (in Japanese), Sep., 1994.

(8) T.MUKAIYAMA, H.OGAWA, Y.YOKOTA, « Development of Integrated Containment and Surveillance System for Fast Critical Facility FCA, - Portal and Penetration Monitors – » , JAERI-Research 98-001, Jan., 1998.

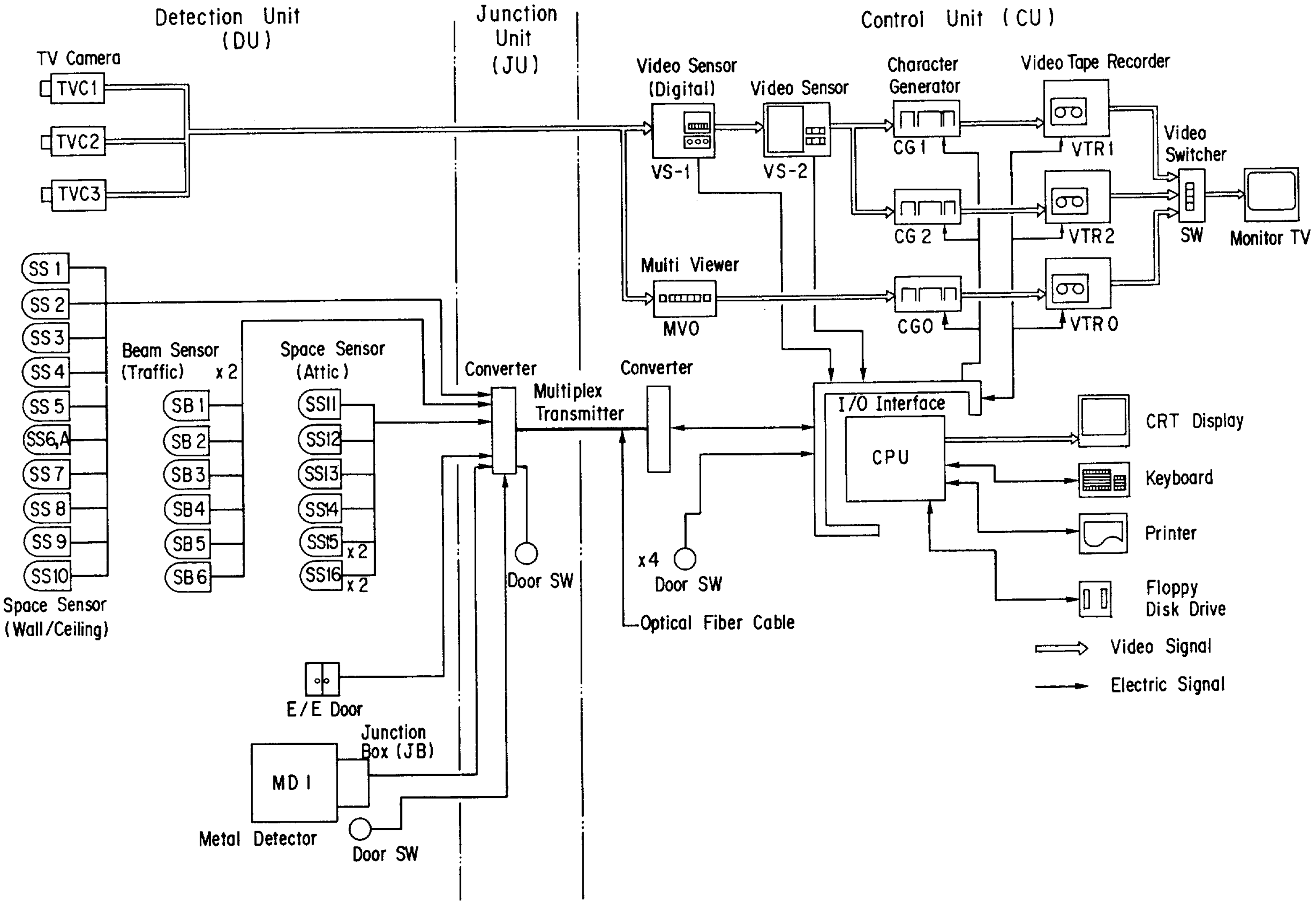


Fig. 1 Conceptual Diagram of Portal Monitor (P/M)

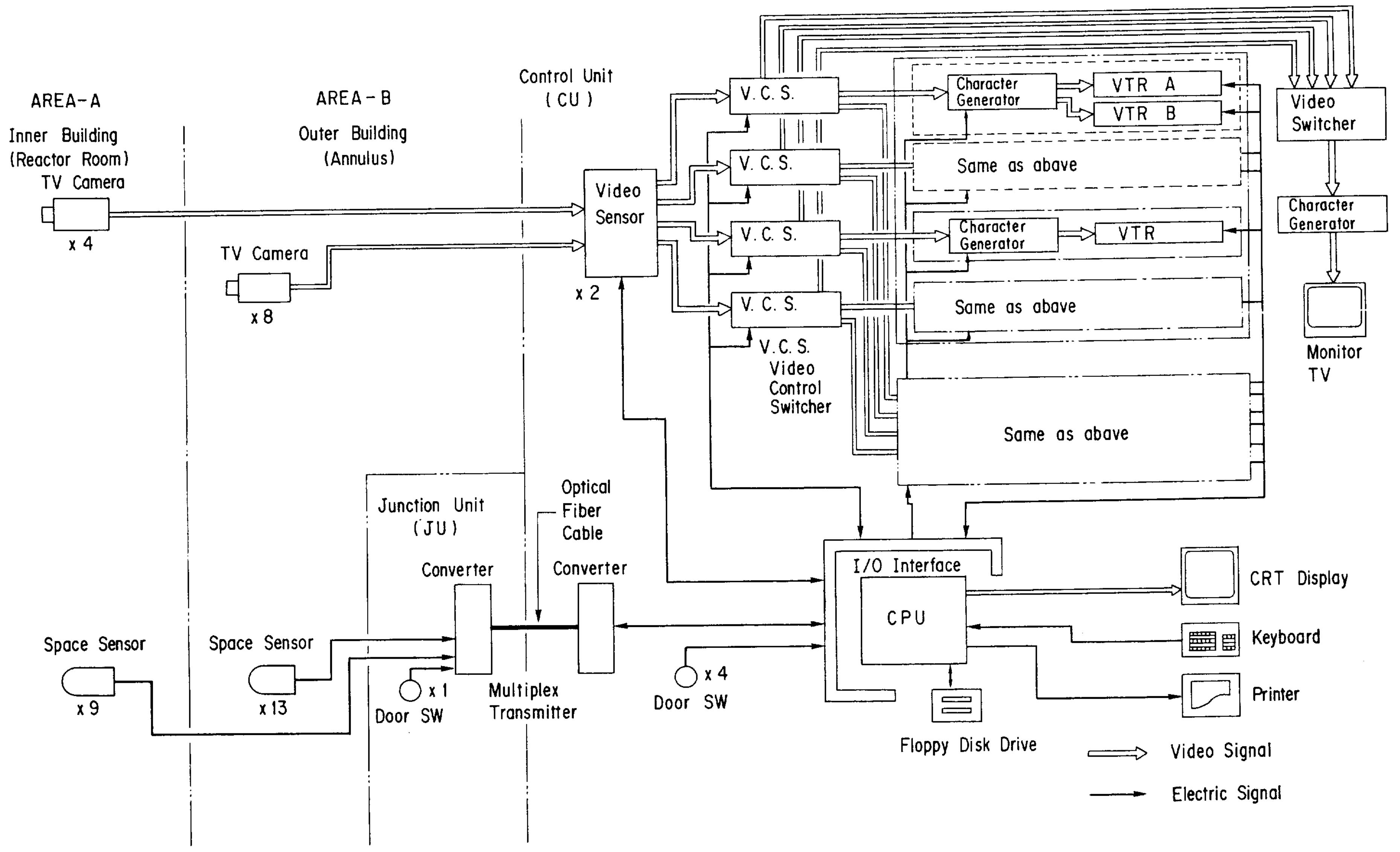


Fig. 2 Conceptual Diagram of Penetration Monitor (PN/M)

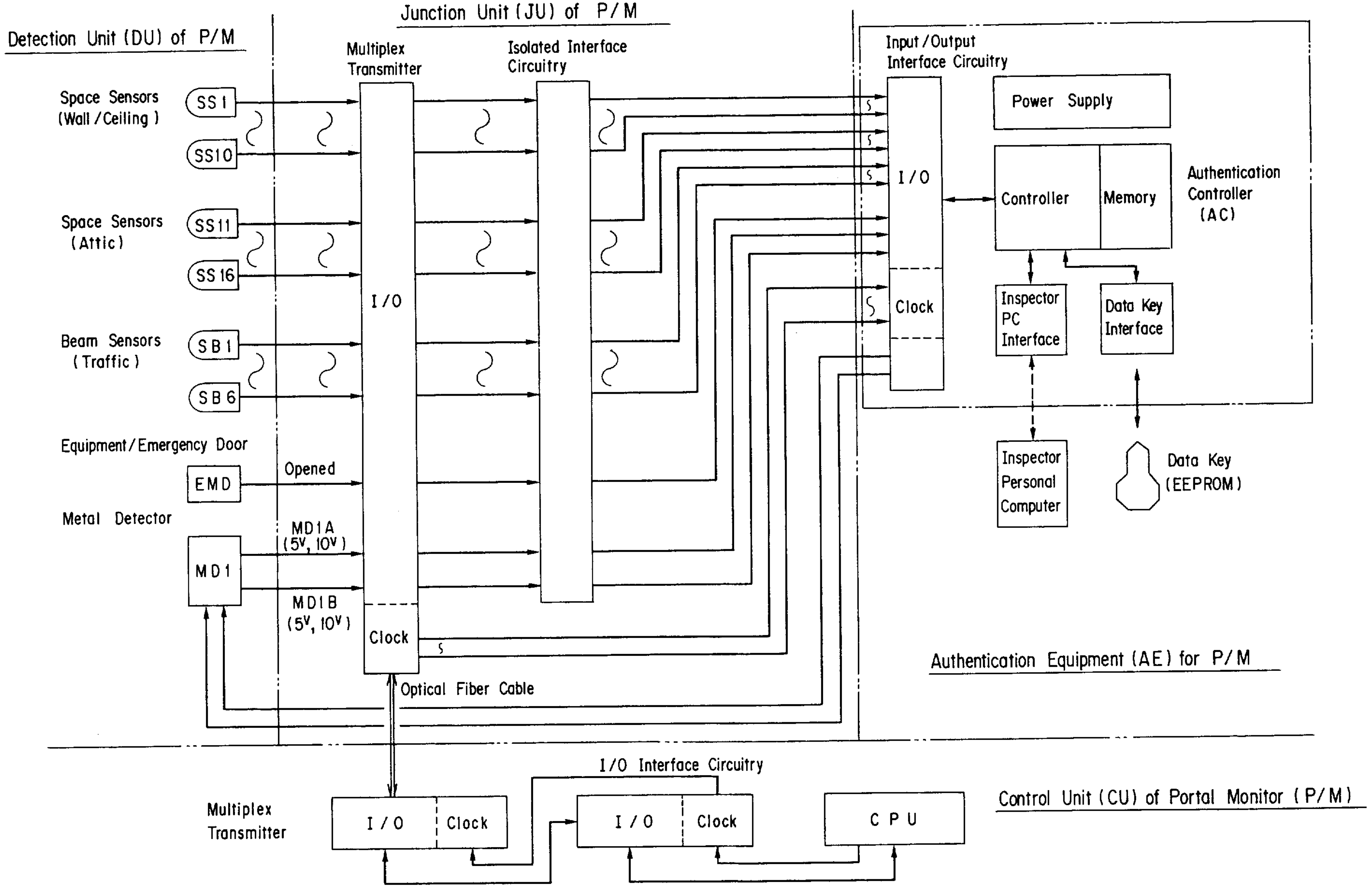


Fig. 3 Block Diagram of FCA Portal Monitor (P/M) with Authentication Equipment (AE)

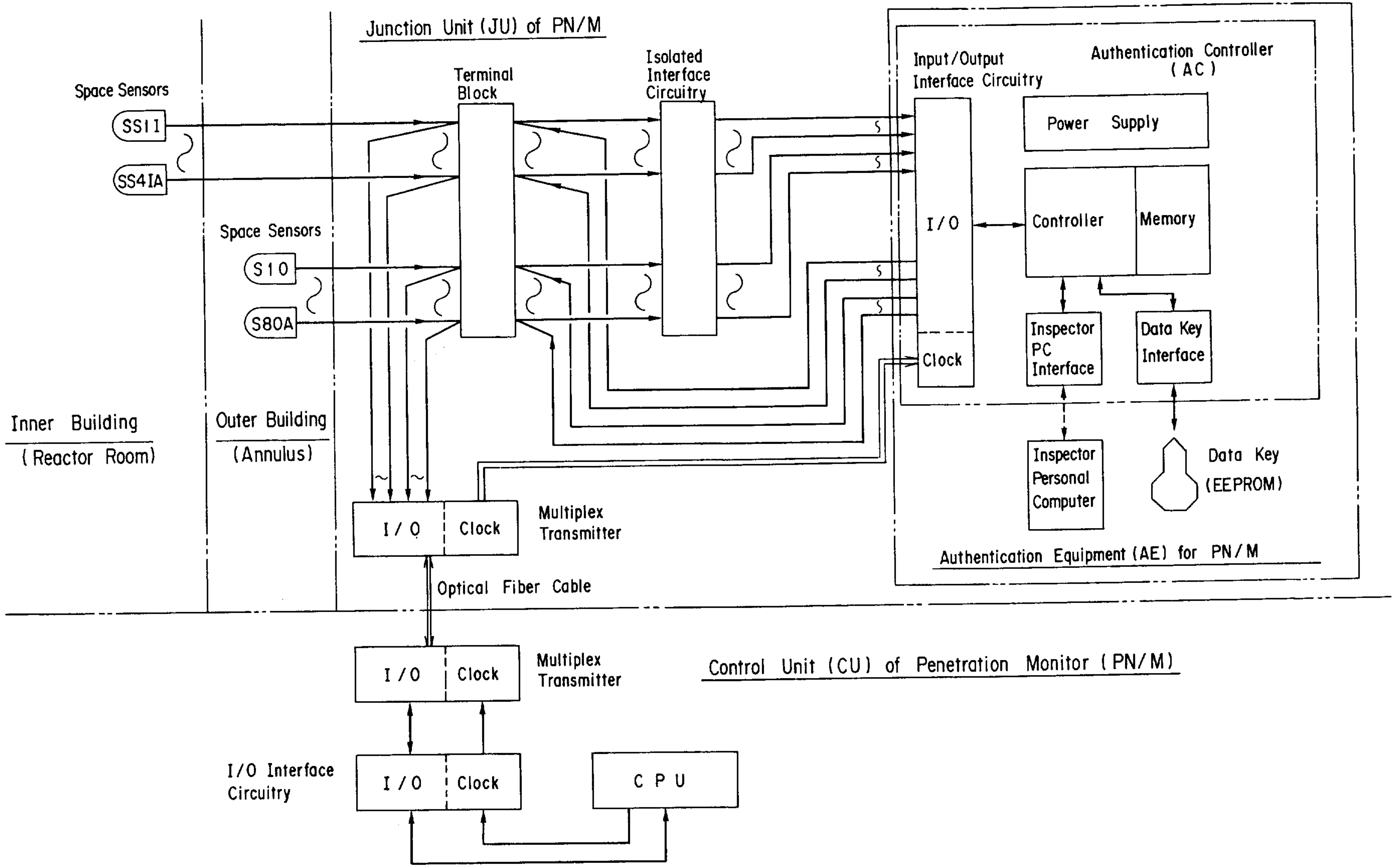


Fig. 4 Block Diagram of FCA Penetration Monitor (PN/M) with Authentication Equipment (AE)

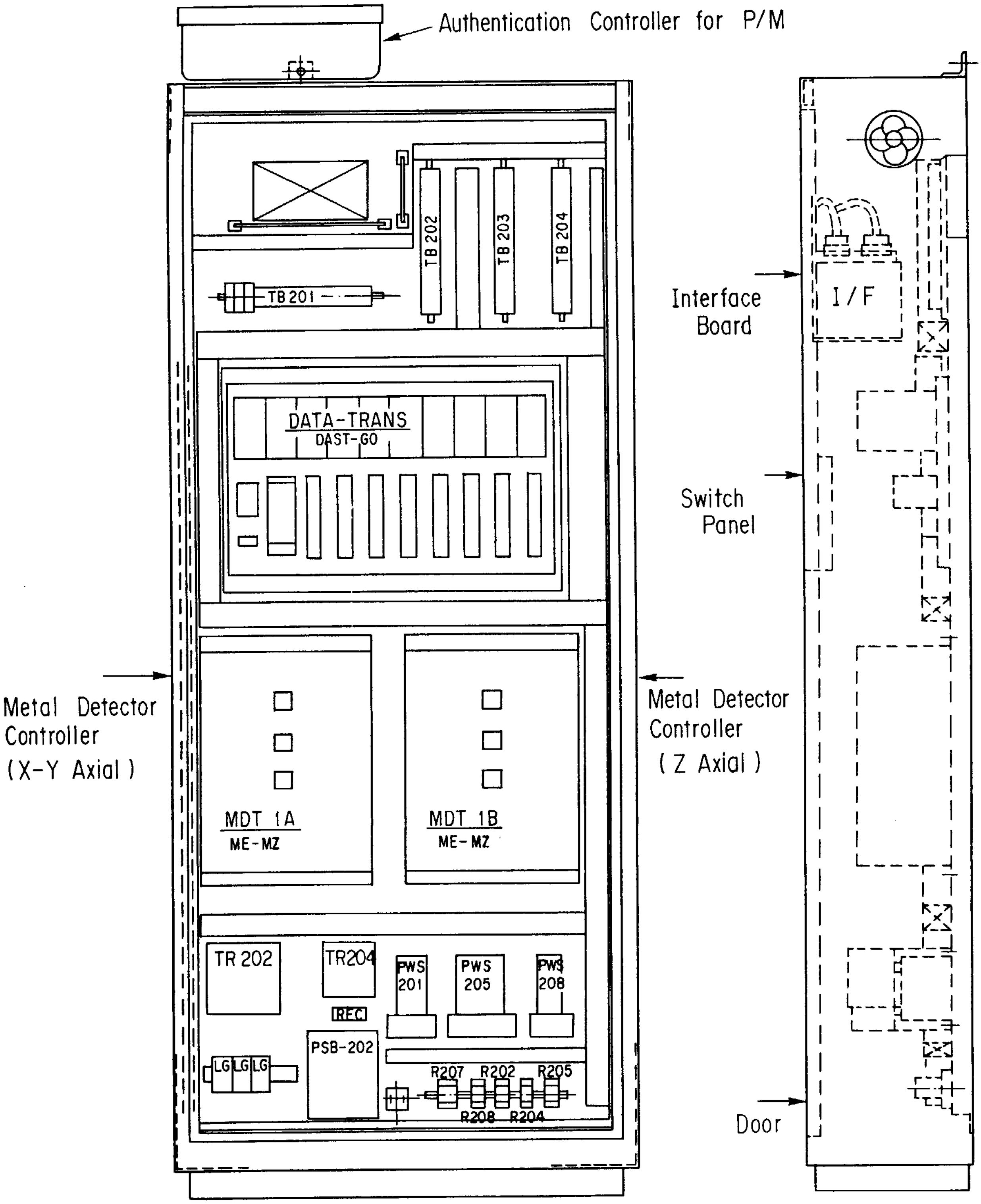
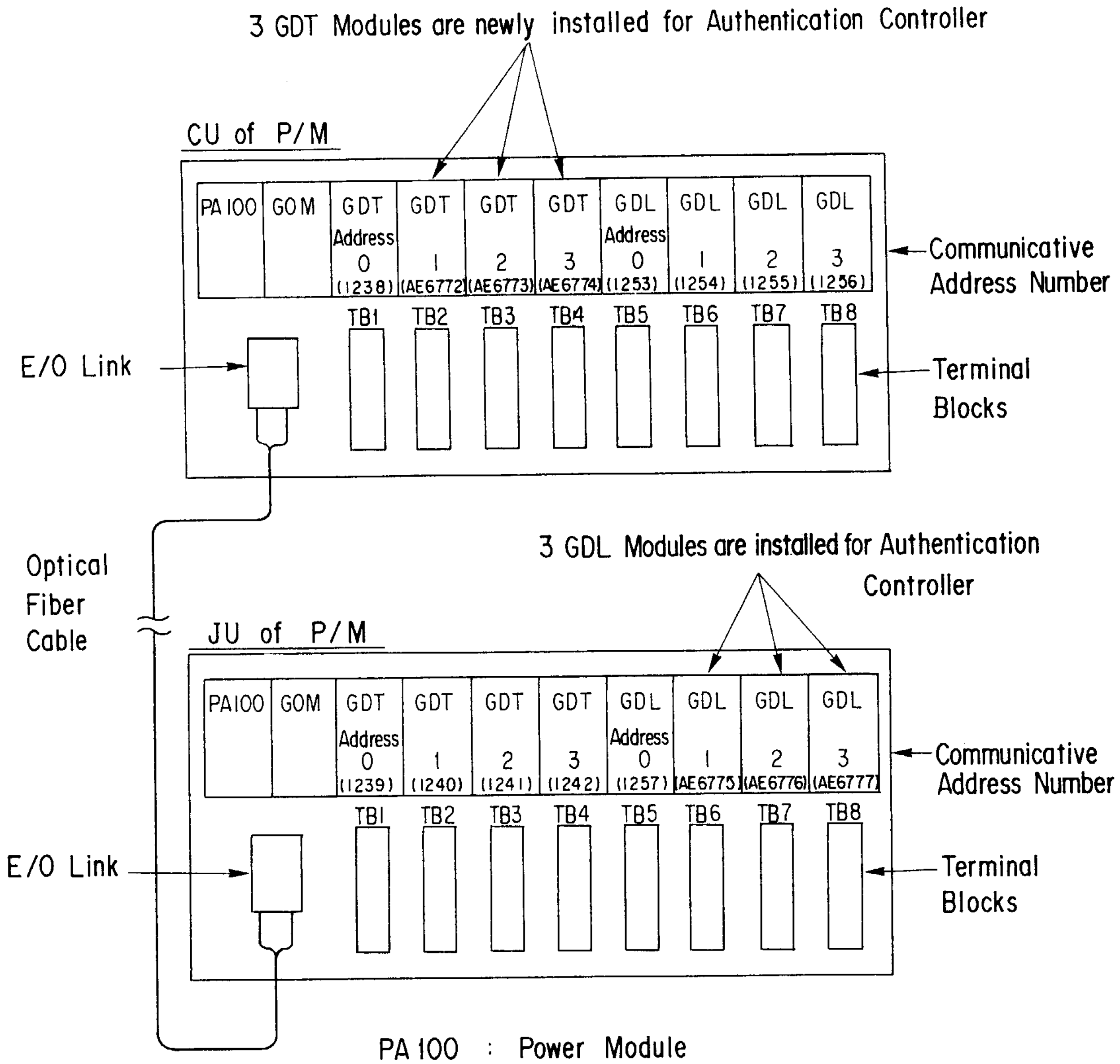


Fig. 5 Junction Unit (JU) of Portal Monitor (P/M)



PA100	:	Power Module
GOM	:	Modem Module
GDT	:	Talker (Output) Module
GDL	:	Listener (Input) Module

CU	:	Control and Recording Unit
JU	:	Junction Unit
P/M	:	Portal Monitor

Fig.6 Multiplex Transmitter Devices of Both CU and JU of P/M

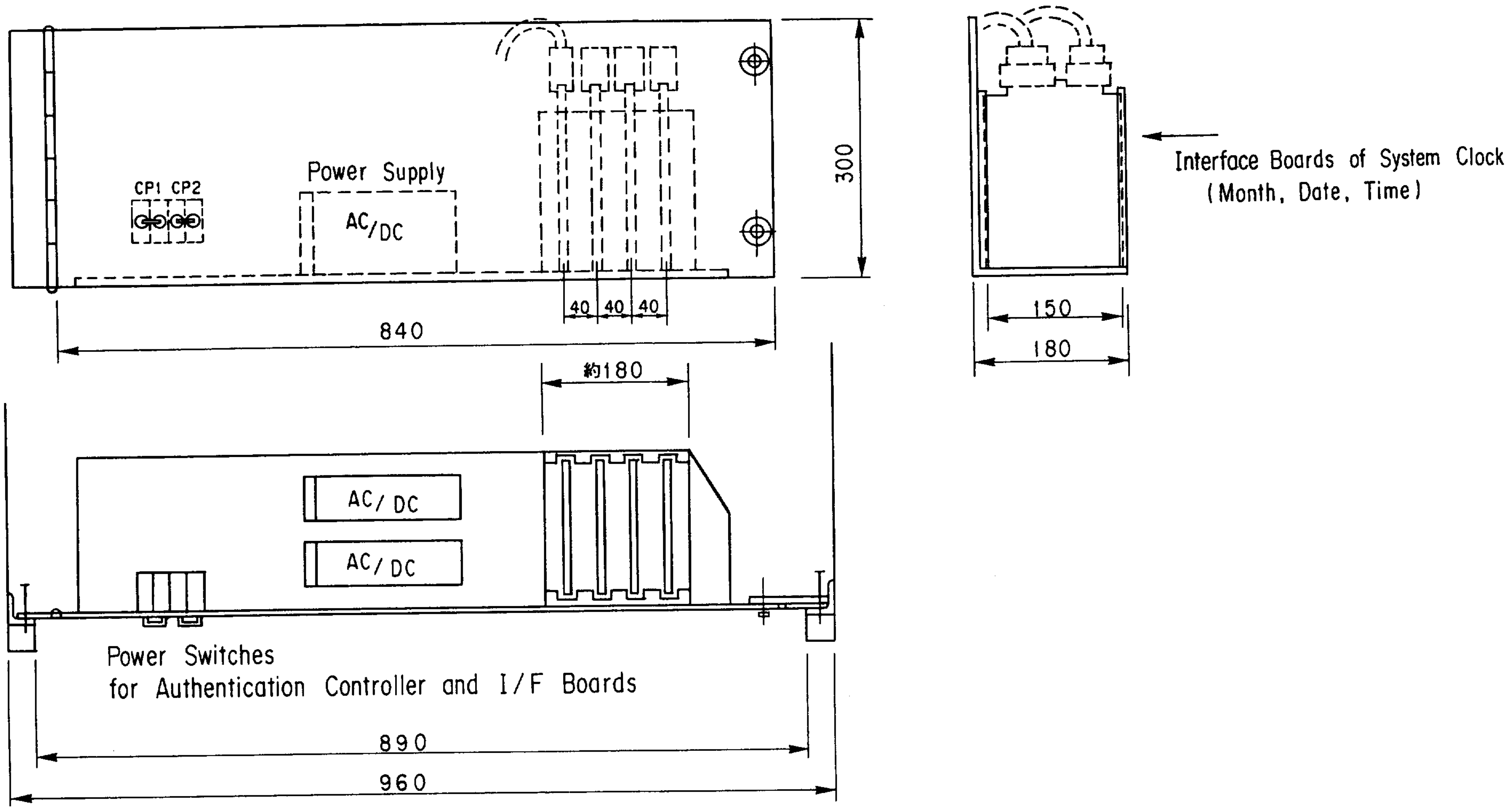


Fig. 7 Interface (I/F) Board Panel of Junction Unit (JU) of P/M

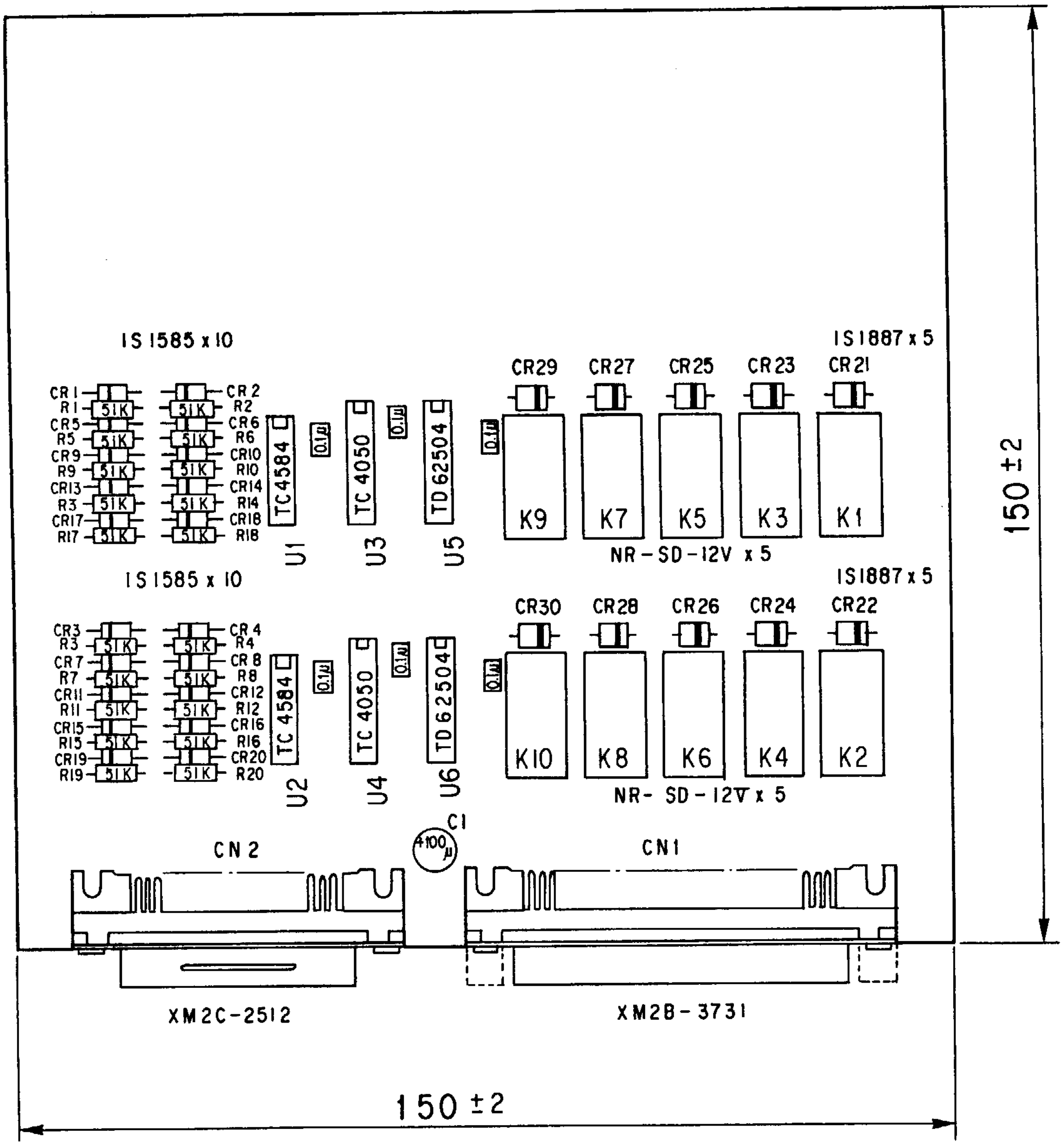


Fig. 8 Interface (I/F) Board for Authentication Equipment (AE)

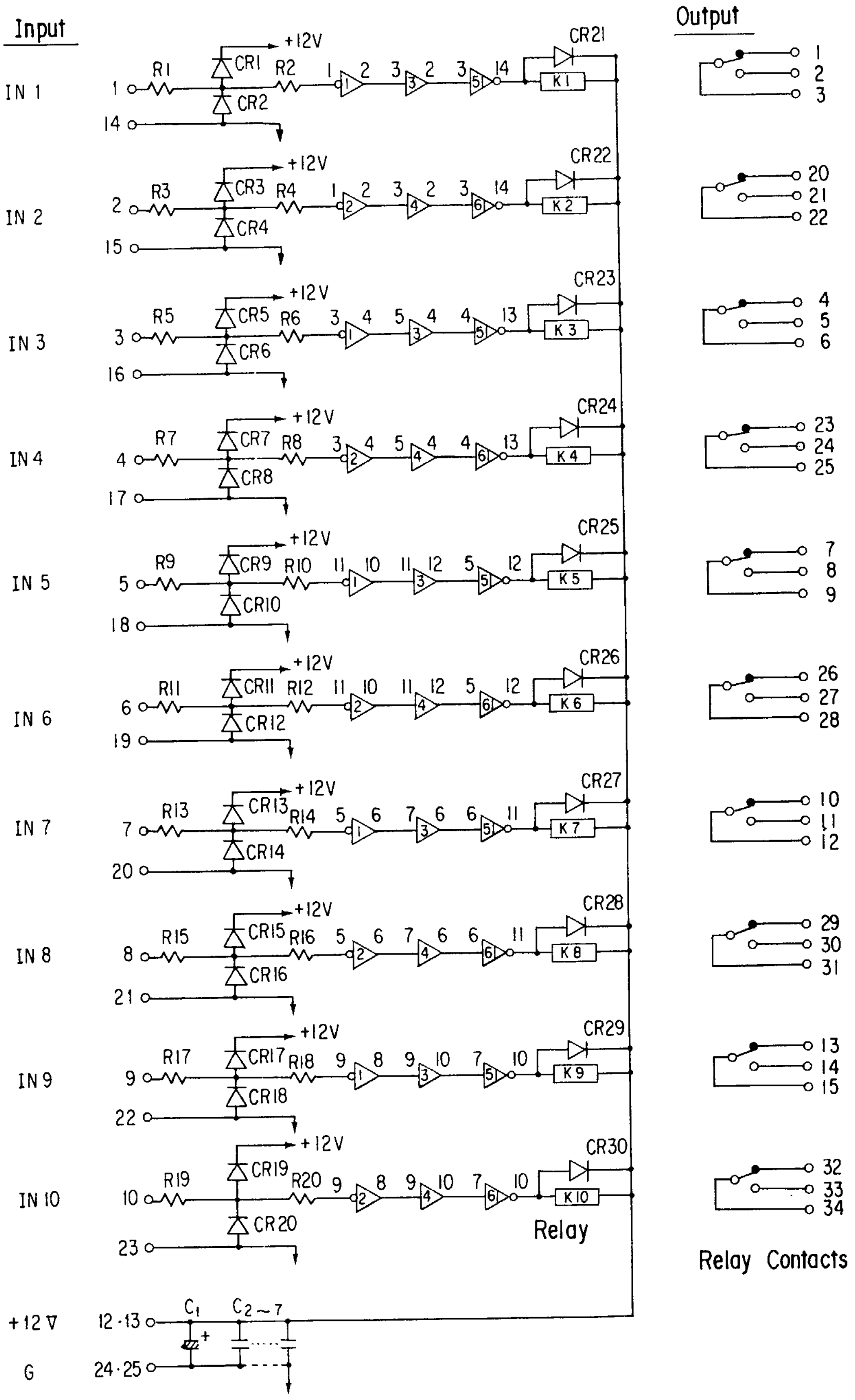


Fig.9 Interface (I/F) Circuitry on the Board for Authentication Equipment (AE)

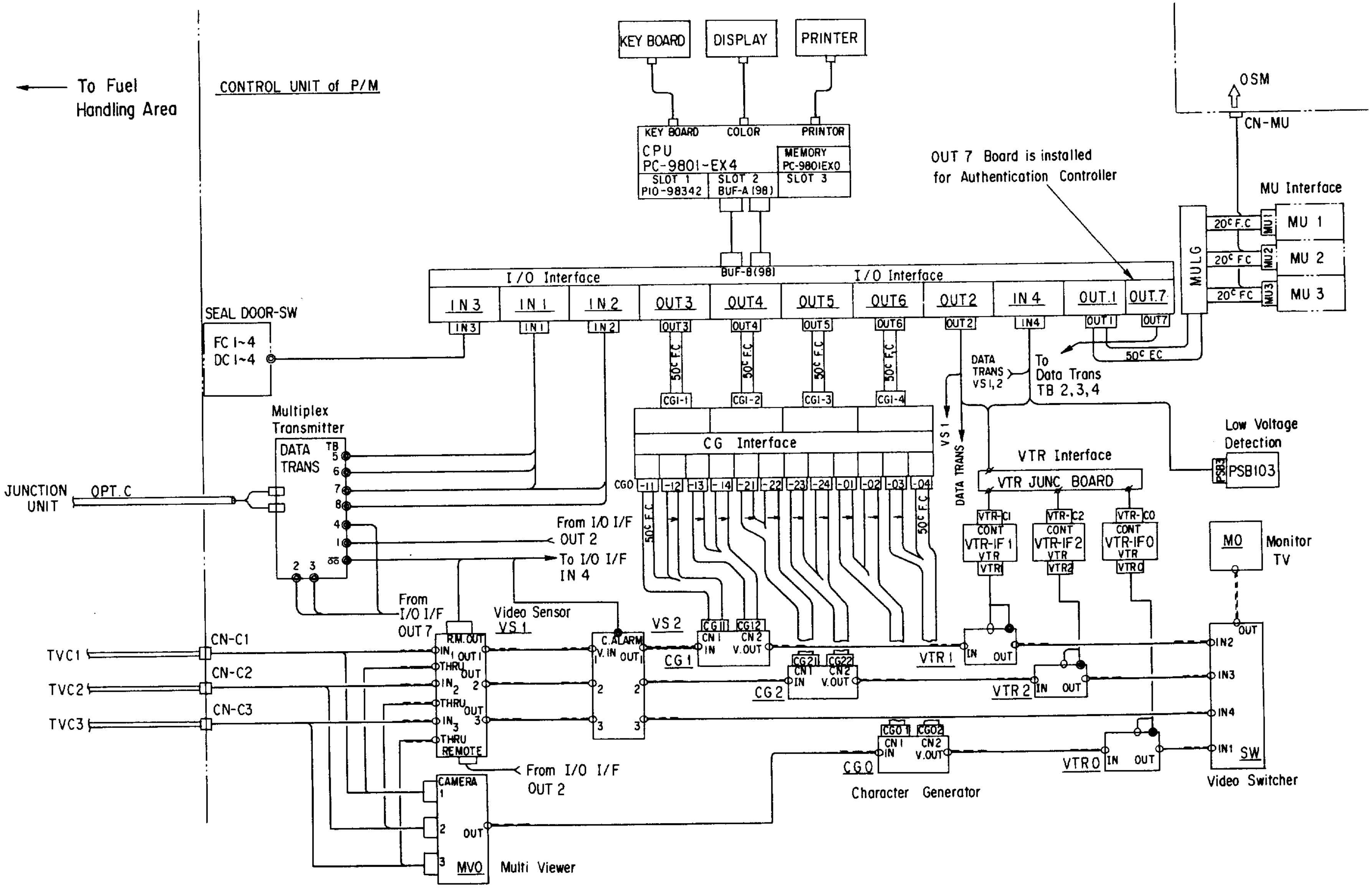


Fig. 10 Wiring Diagram of Control Unit (CU of P/M)

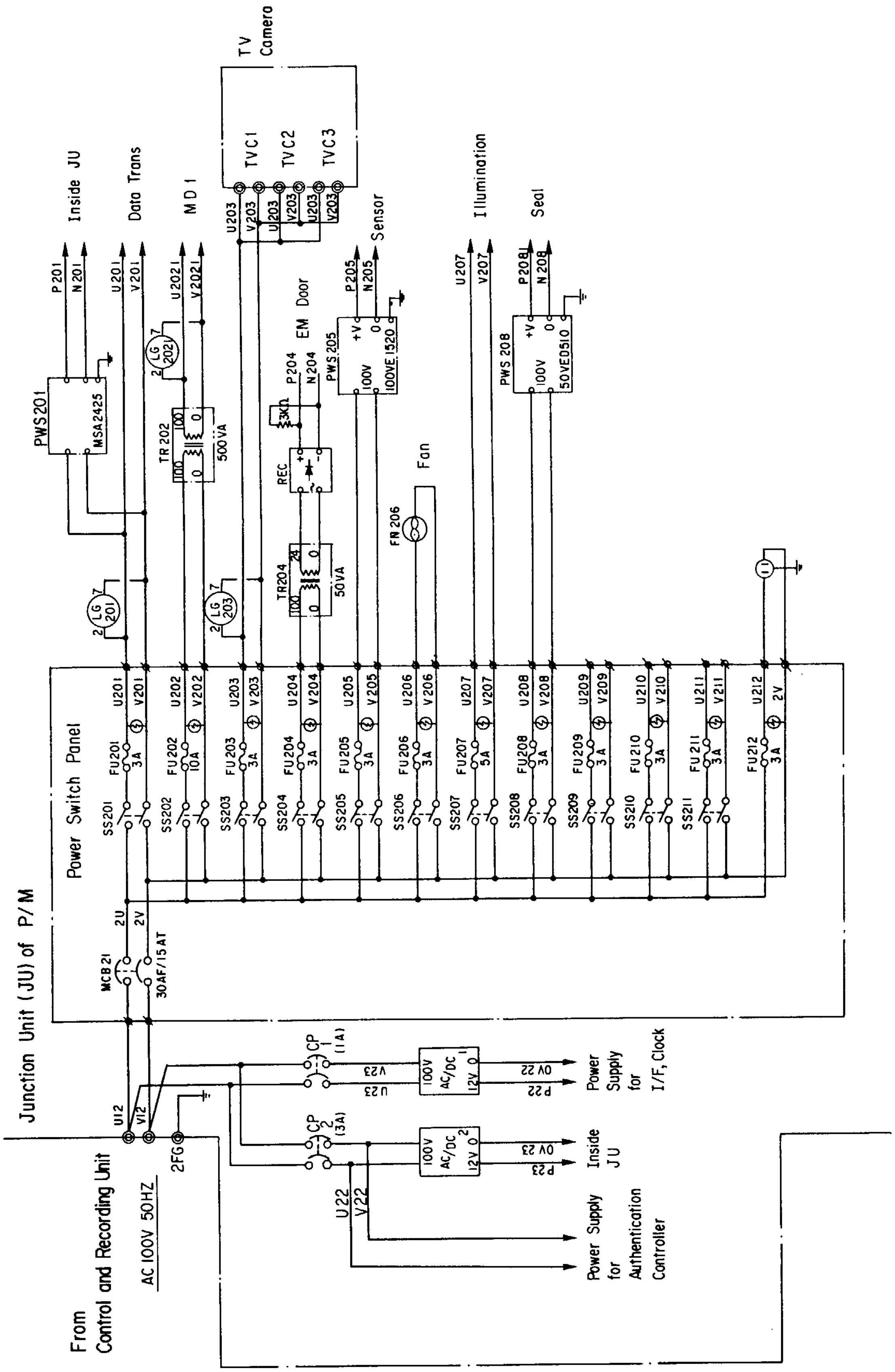
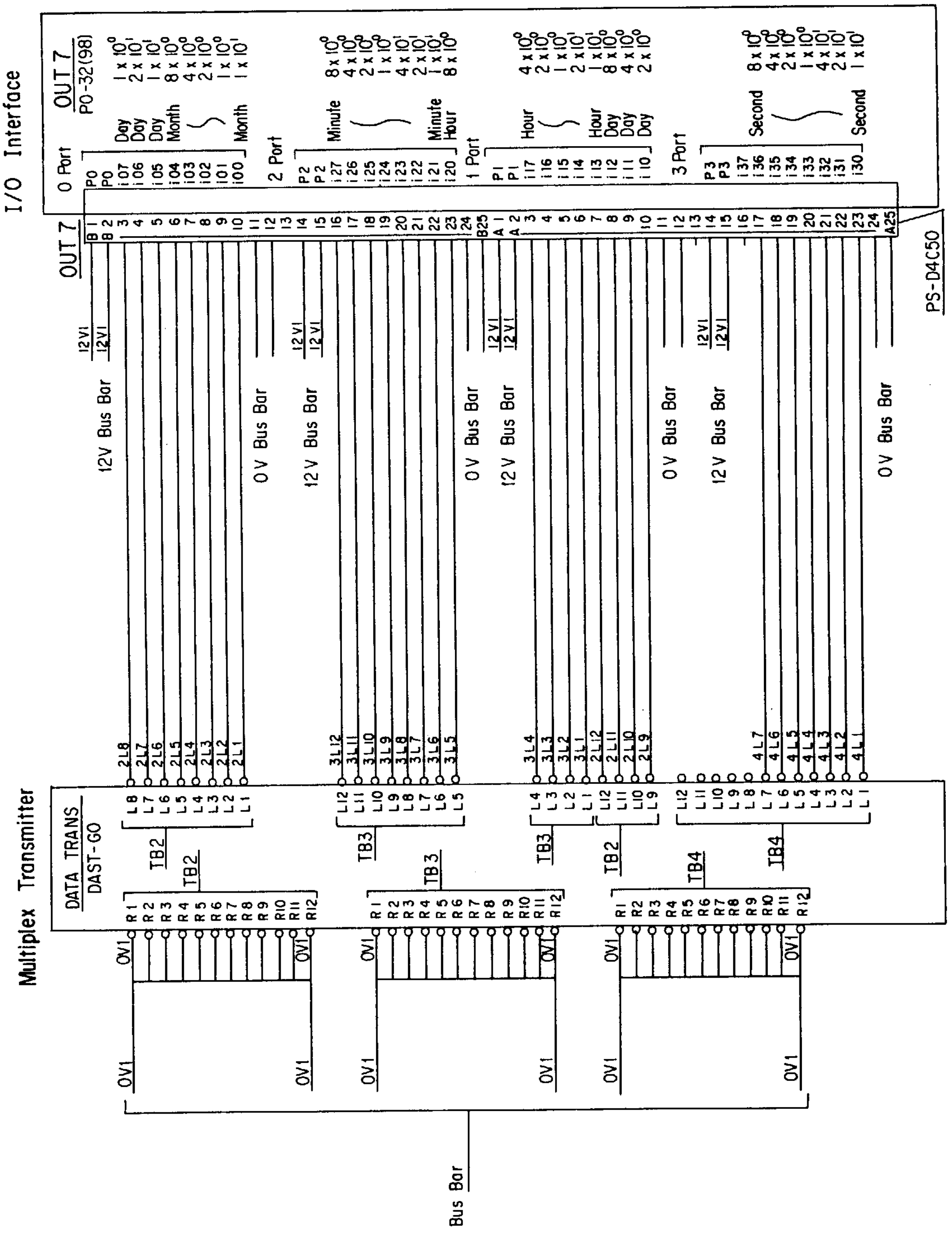


Fig. 11 Power Supply of Junction Unit (JU of P/M)



Control Unit (CU) of Portal Monitor (P/M)

Fig. 12 Clock Signals for Authentication Controller (AC of P/M) (1/3)

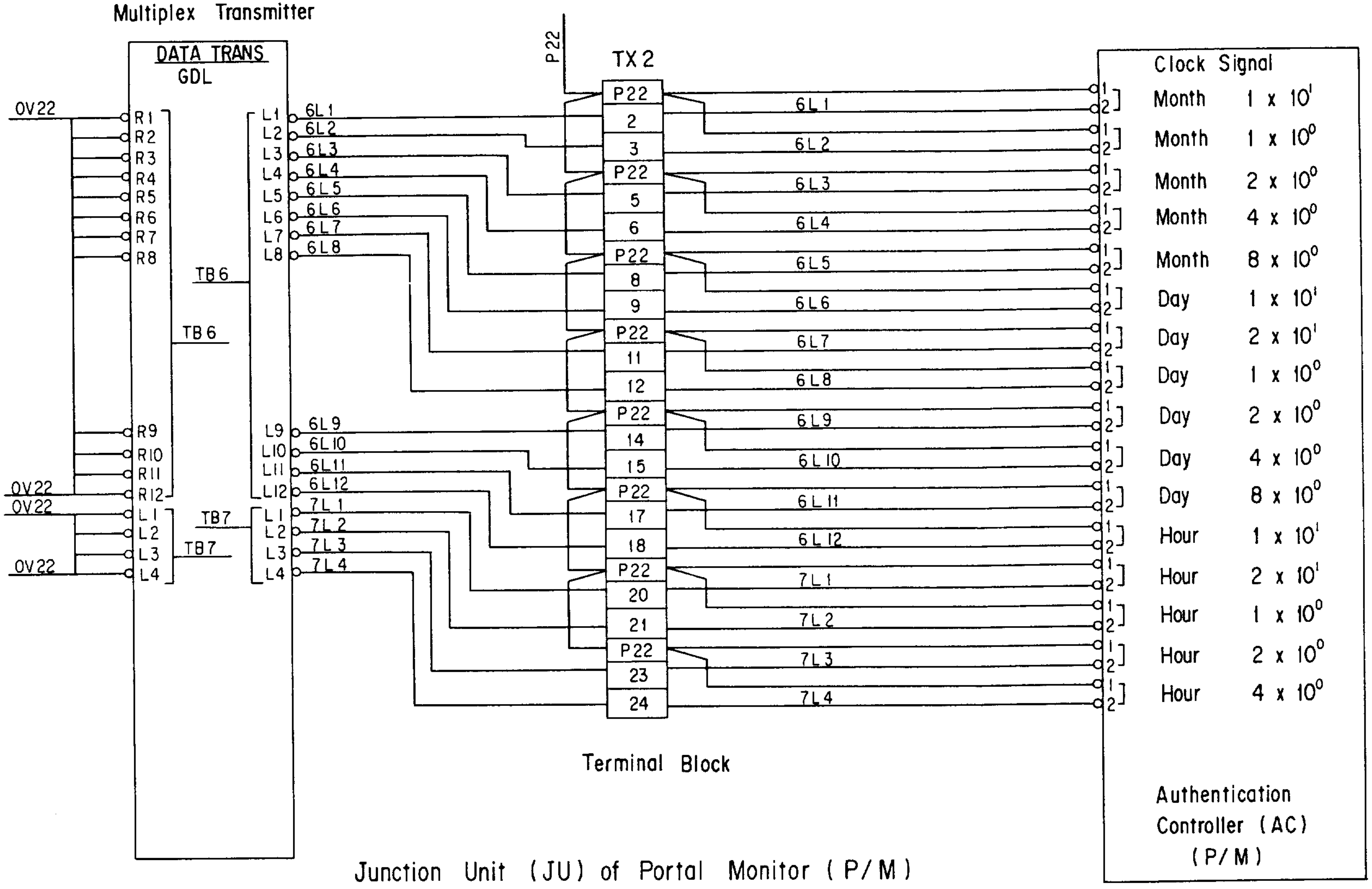
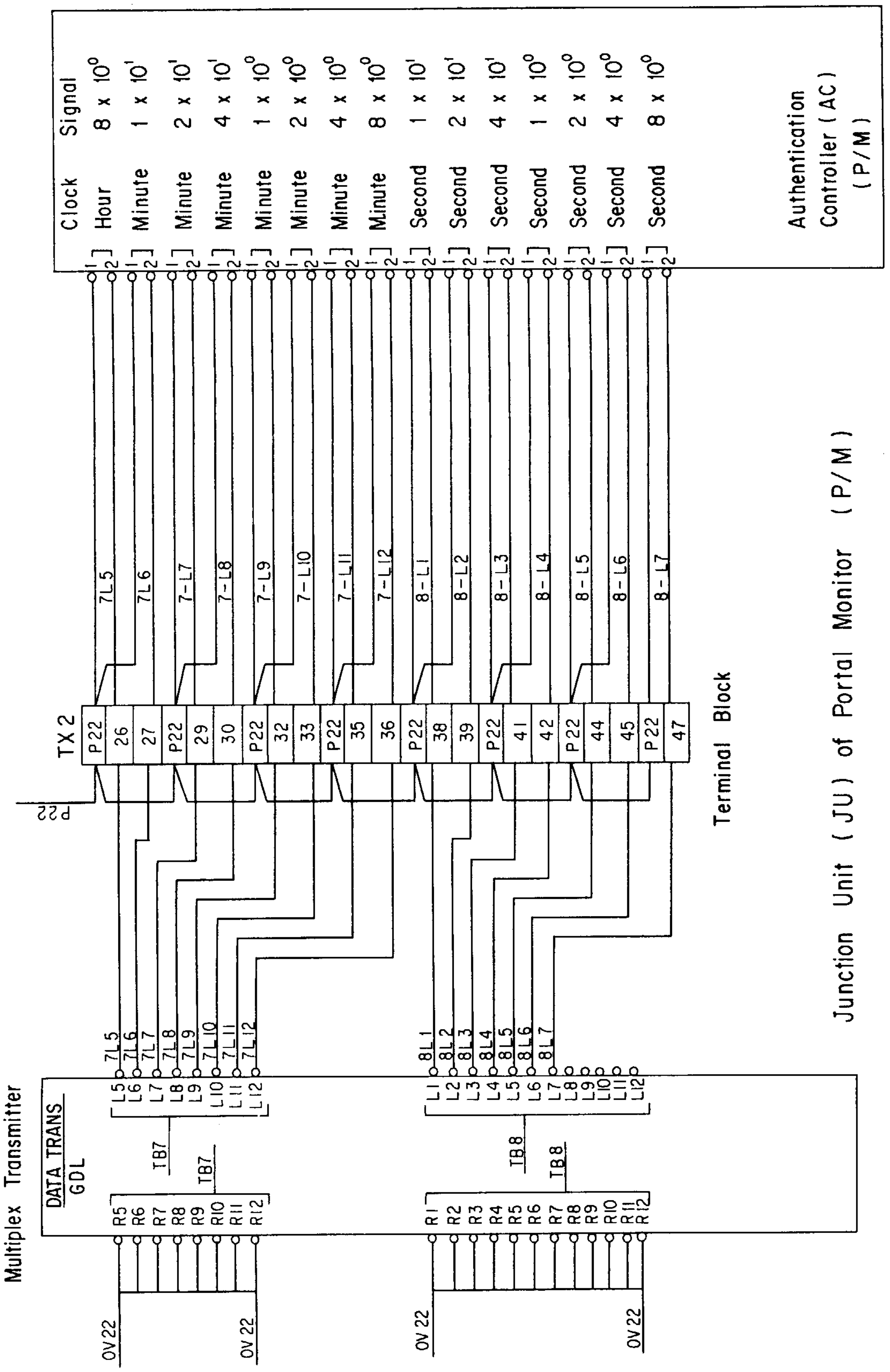
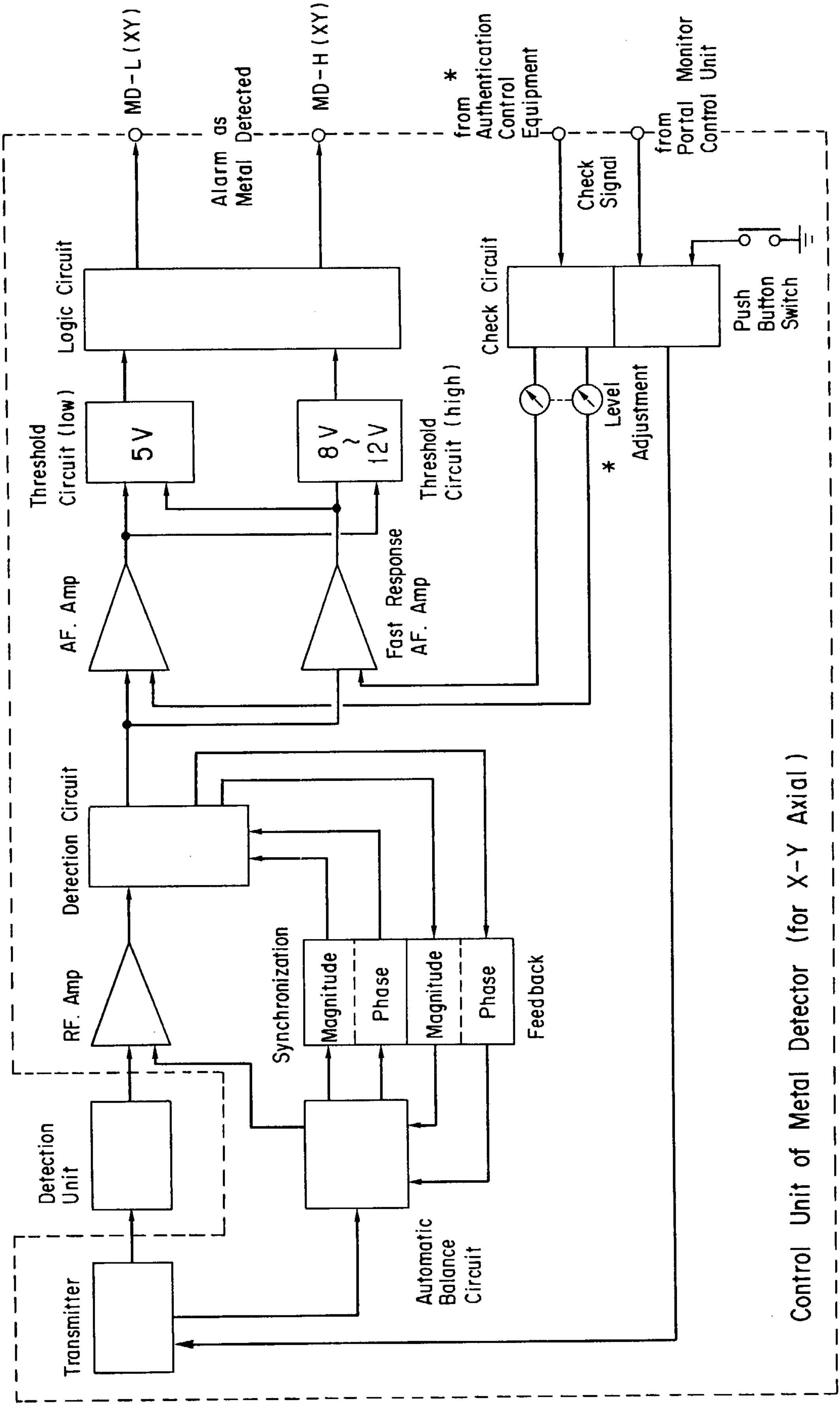


Fig. 13 Clock Signals for Authentication Controller (AC of P/M) (2/3)


Multiplex Transmitter
DATA TRANS
GDL
TB7
TB8
L5 L6 L7 L8 L9 L10 L11 L12
R5 R6 R7 R8 R9 R10 R11 R12
L1 L2 L3 L4 L5 L6 L7 L8 L9 L10 L11 L12
R1 R2 R3 R4 R5 R6 R7 R8 R9 R10 R11 R12
7L5 7L6 7L7 7L8 7L9 7L10 7L11 7L12
8L1 8L2 8L3 8L4 8L5 8L6 8L7
OV22
P22
TX2
P22 26 27 P22 29 30 P22 32 33 P22 35 36 P22 38 39 P22 41 42 P22 44 45 P22 47
Terminal Block
7L5 7L6 7-L7 7-L8 7-L9 7-L10 7-L11 7-L12 8-L1 8-L2 8-L3 8-L4 8-L5 8-L6 8-L7
Clock Signal
Hour 8 x 10^0
Minute 1 x 10^1
Minute 2 x 10^1
Minute 4 x 10^1
Minute 1 x 10^0
Minute 2 x 10^0
Minute 4 x 10^0
Minute 8 x 10^0
Second 1 x 10^1
Second 2 x 10^1
Second 4 x 10^1
Second 1 x 10^0
Second 2 x 10^0
Second 4 x 10^0
Second 8 x 10^0
1 2
Authentication Controller (AC) (P/M)

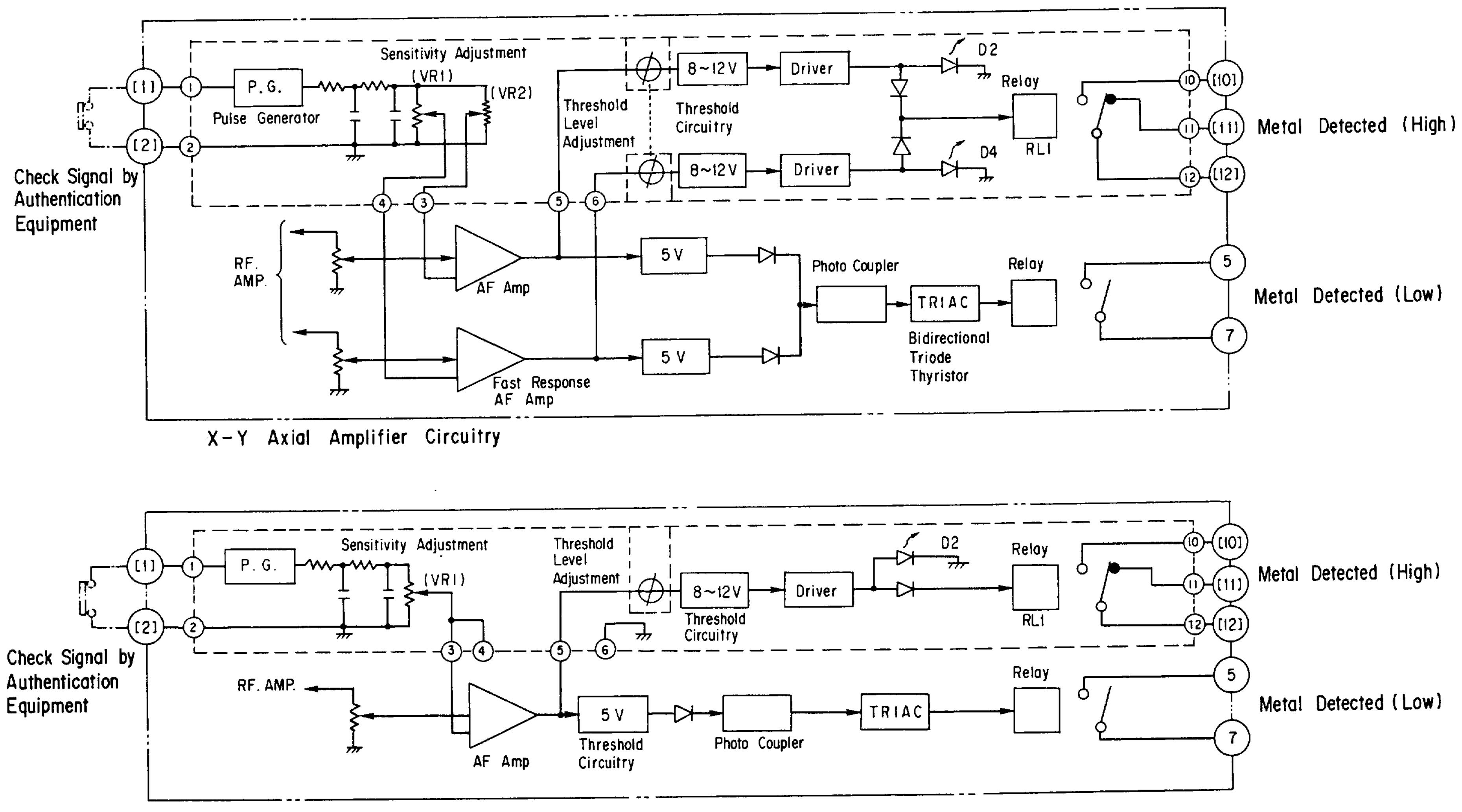
Junction Unit (JU) of Portal Monitor (P/M)

Fig. 14 Clock Signals for Authentication Controller (AC of P/M) (3/3)



* Added and Modified Circuitry for Authentication Equipment

Fig.15 System Block Diagram (X-Y Axial) of Metal Detector (MD1)



X-Y Axial Amplifier Circuitry

Z Axial Amplifier Circutry

Note : Circuitries within chained-line is revised and is made new one for the installation of Authentication Equipment.

Fig. 16 Metal-Detected Circuitry (X-Y, Z Axial) of Metal Detector (MD1)

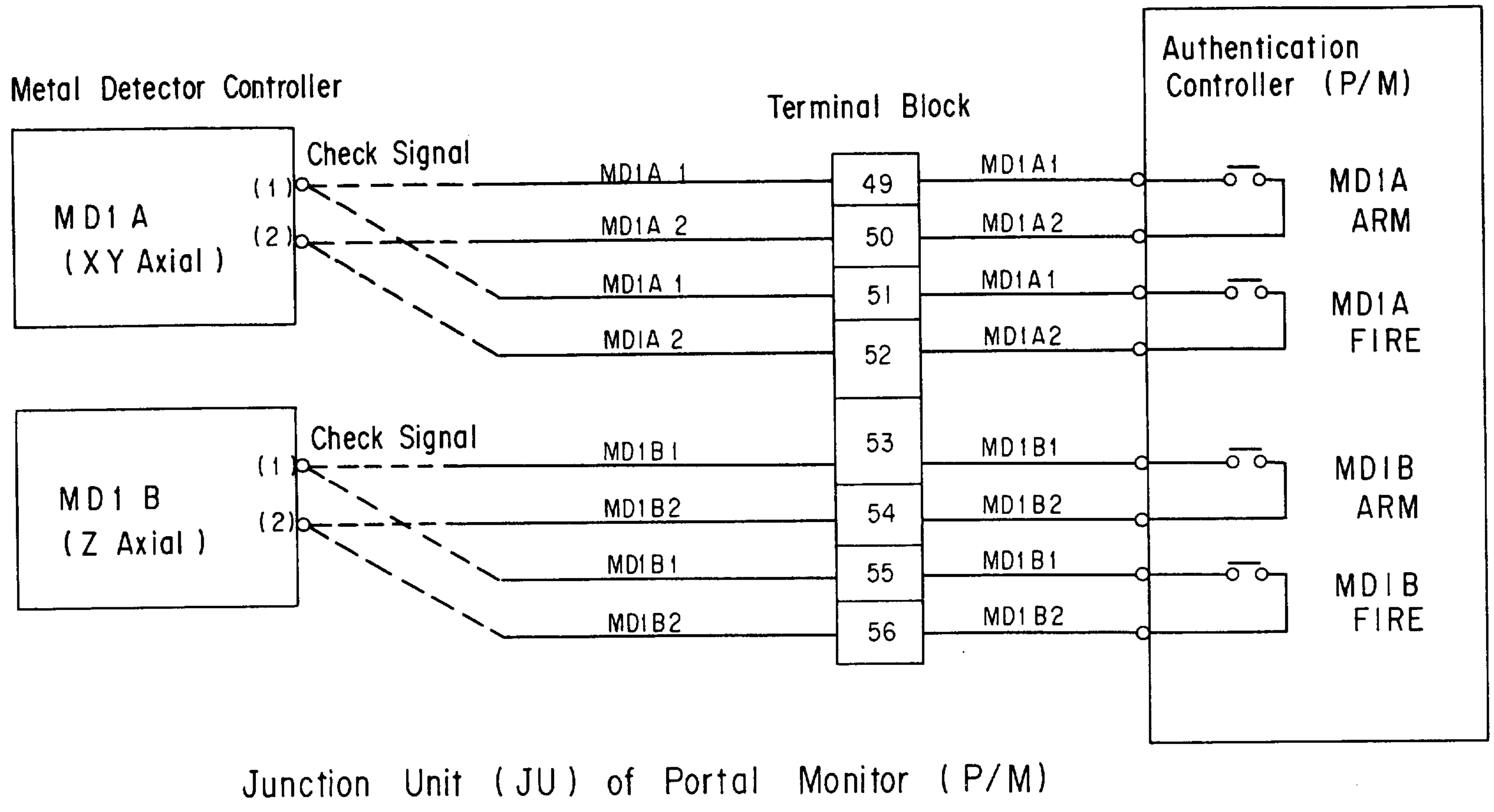


Fig . 17 Check Signal to Metal Detector (MD1) by means of Authentication Controller (AC of P/M)

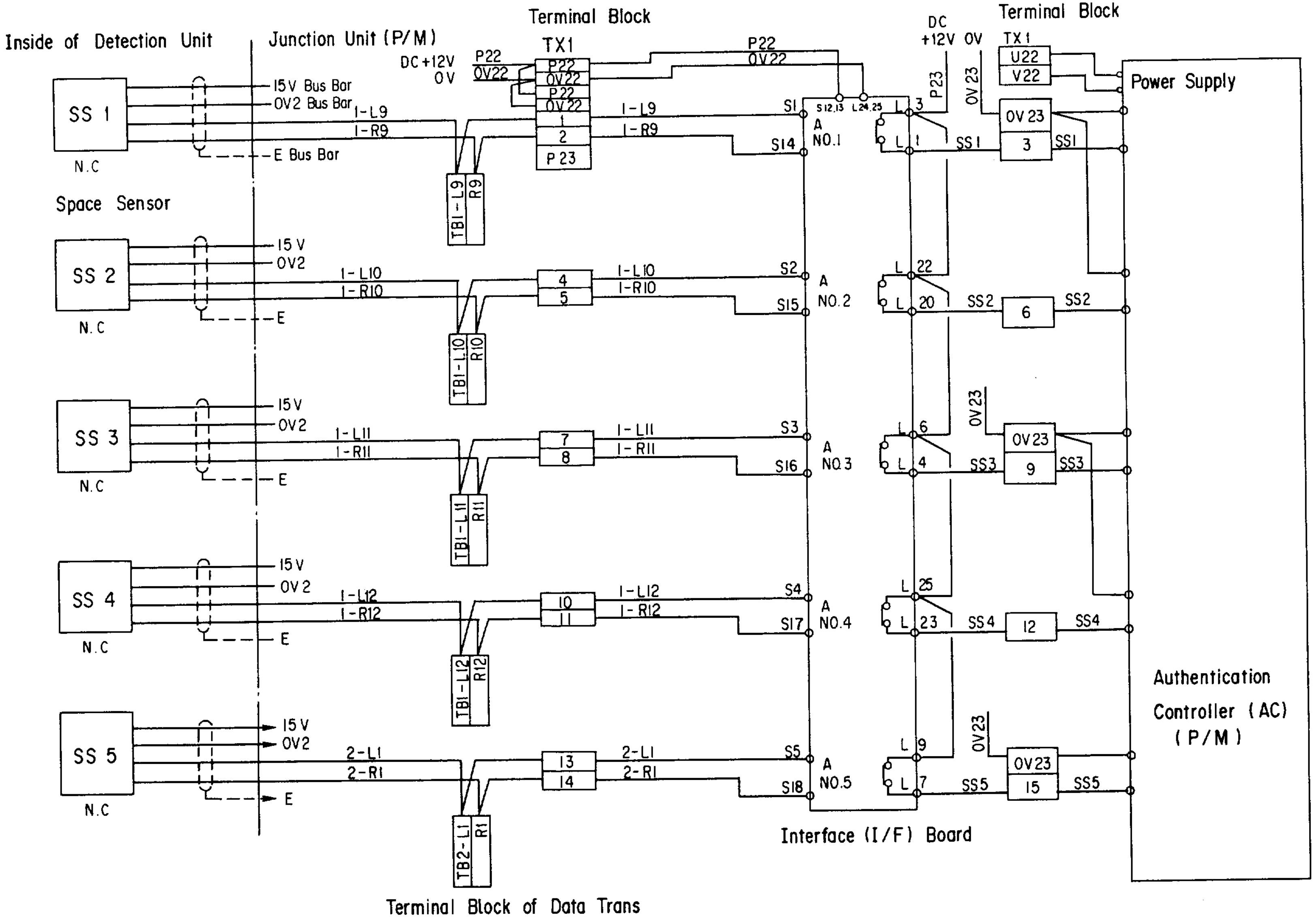


Fig. 18 Sensor Signals for Authentication Controller (AC of P/M) (1/6)

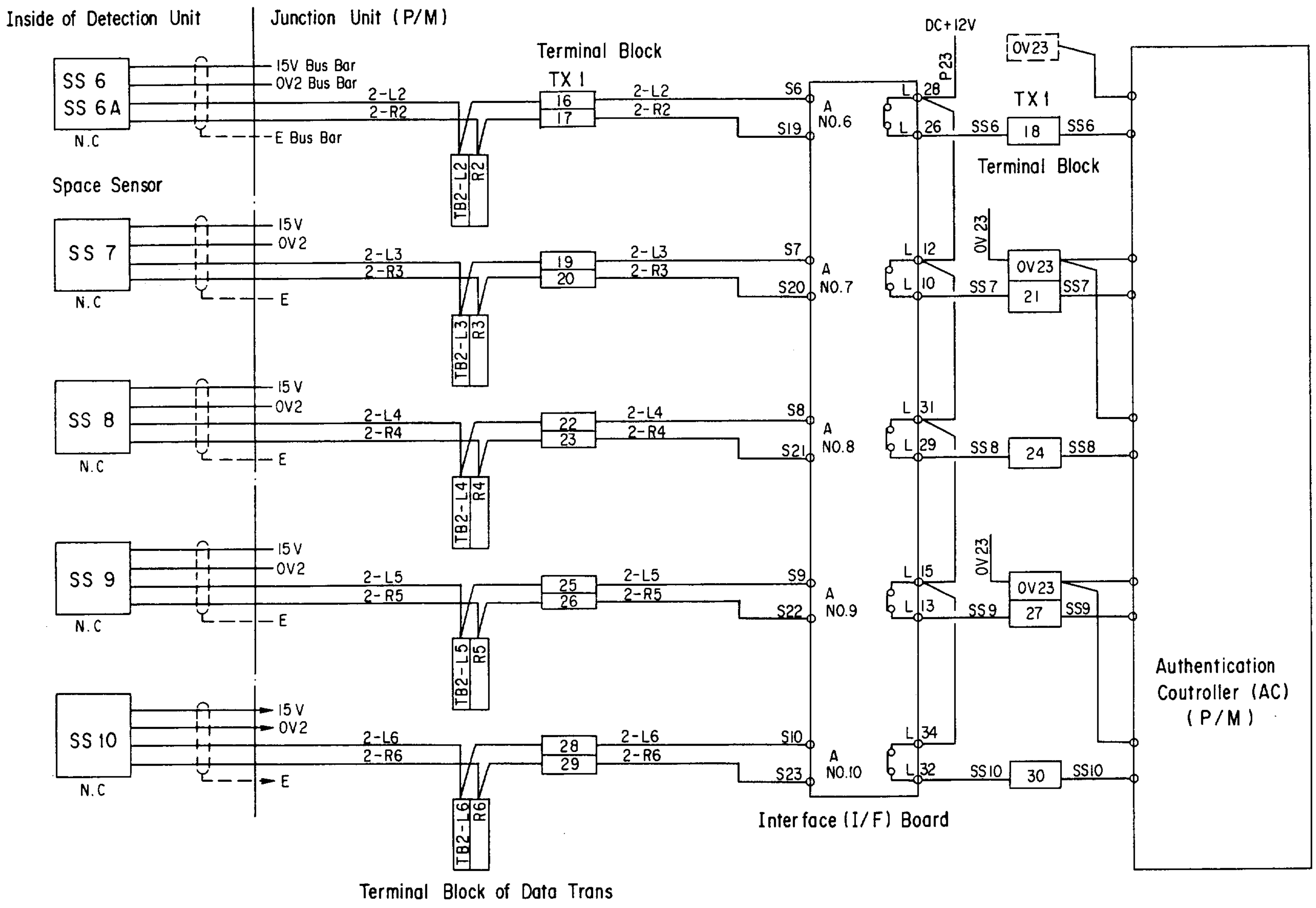


Fig. 19 Sensor Signals for Authentication Controller (AC of P/M) (2/6)

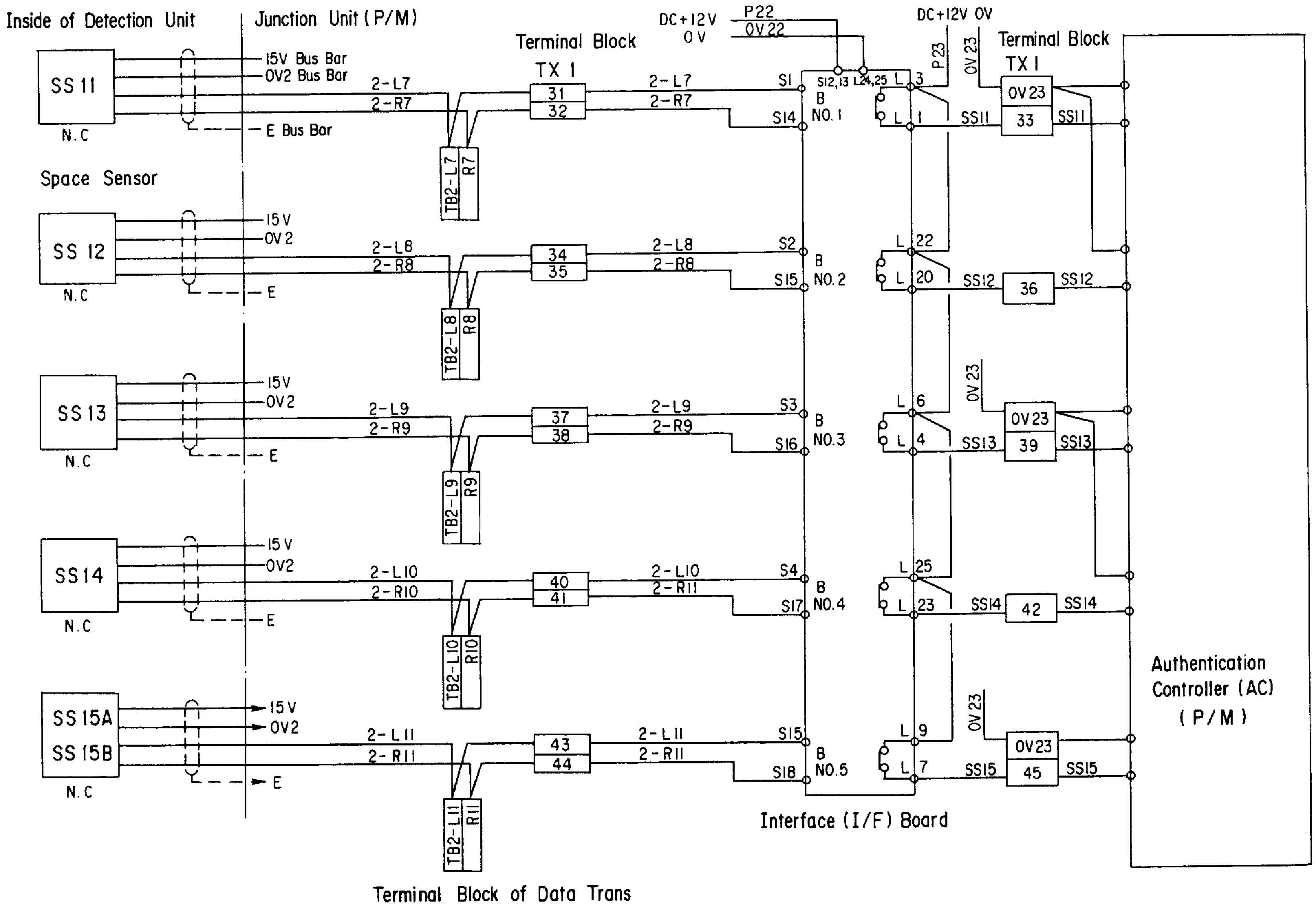


Fig. 20 Sensor Signals for Authentication Controller (AC of P/M) (3/6)

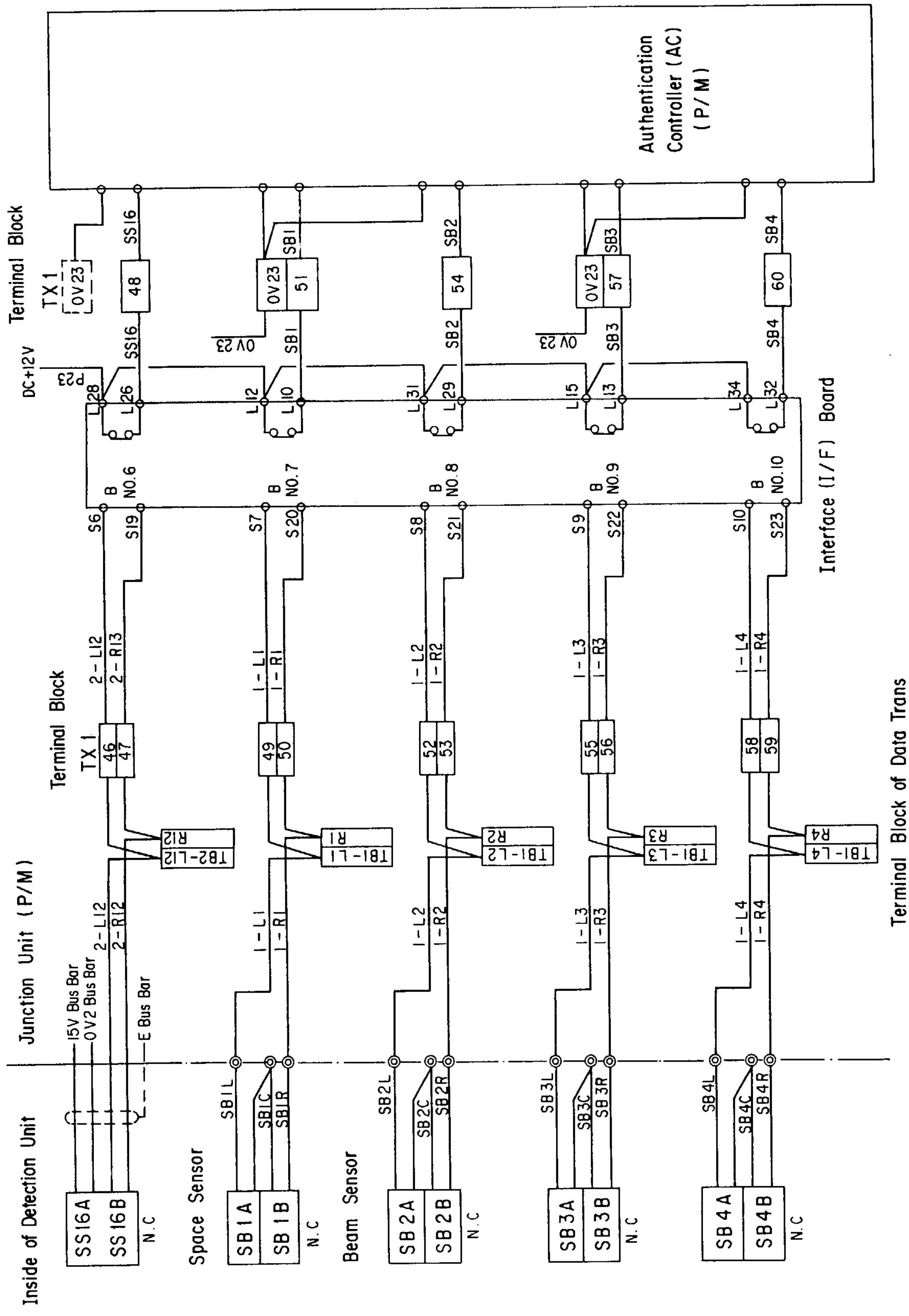


Fig. 21 Sensor Signals for Authentication Controller (AC of P/M) (4/6)

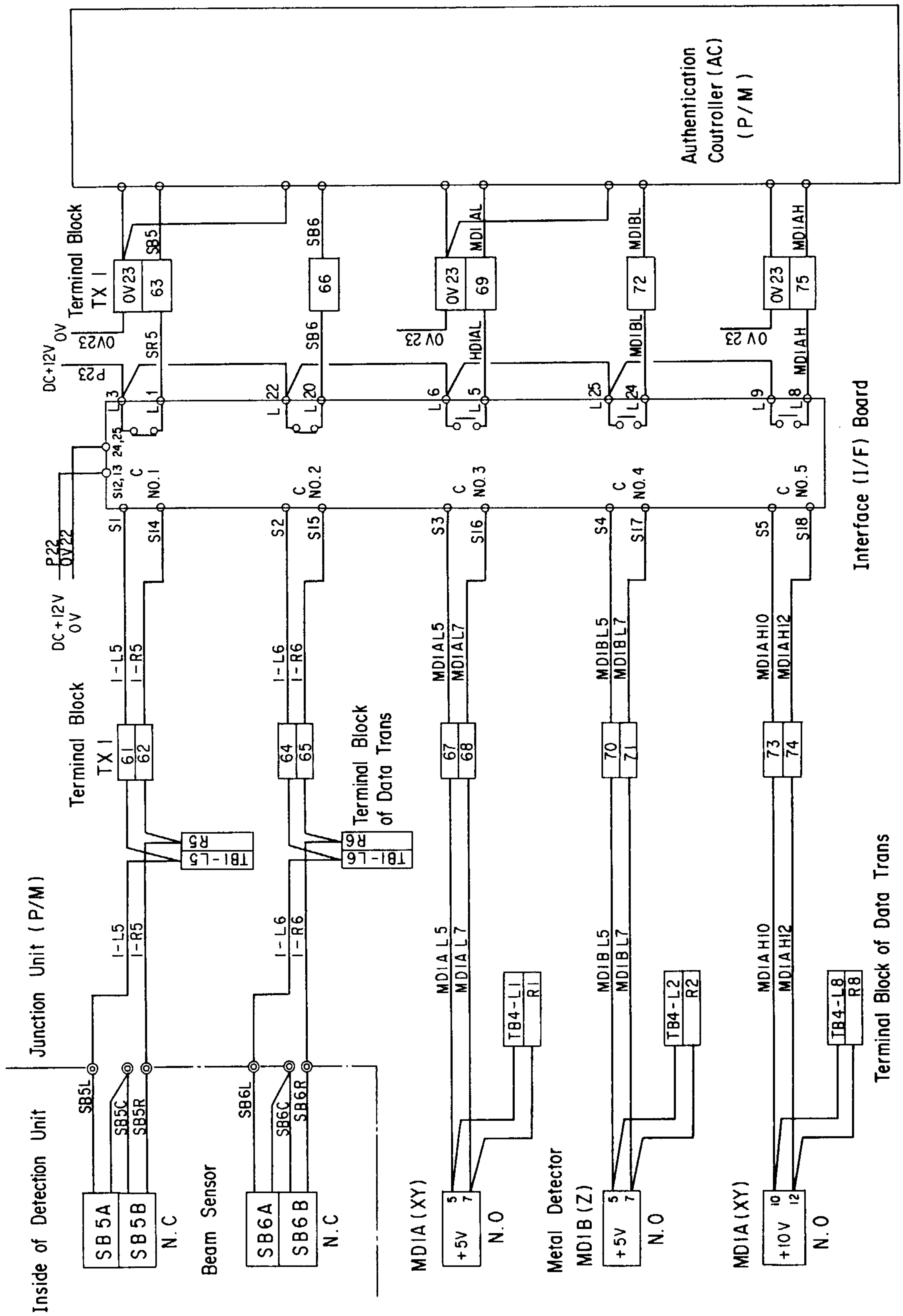


Fig. 22 Sensor Signals for Authentication Controller (AC of P/M) (5/6)

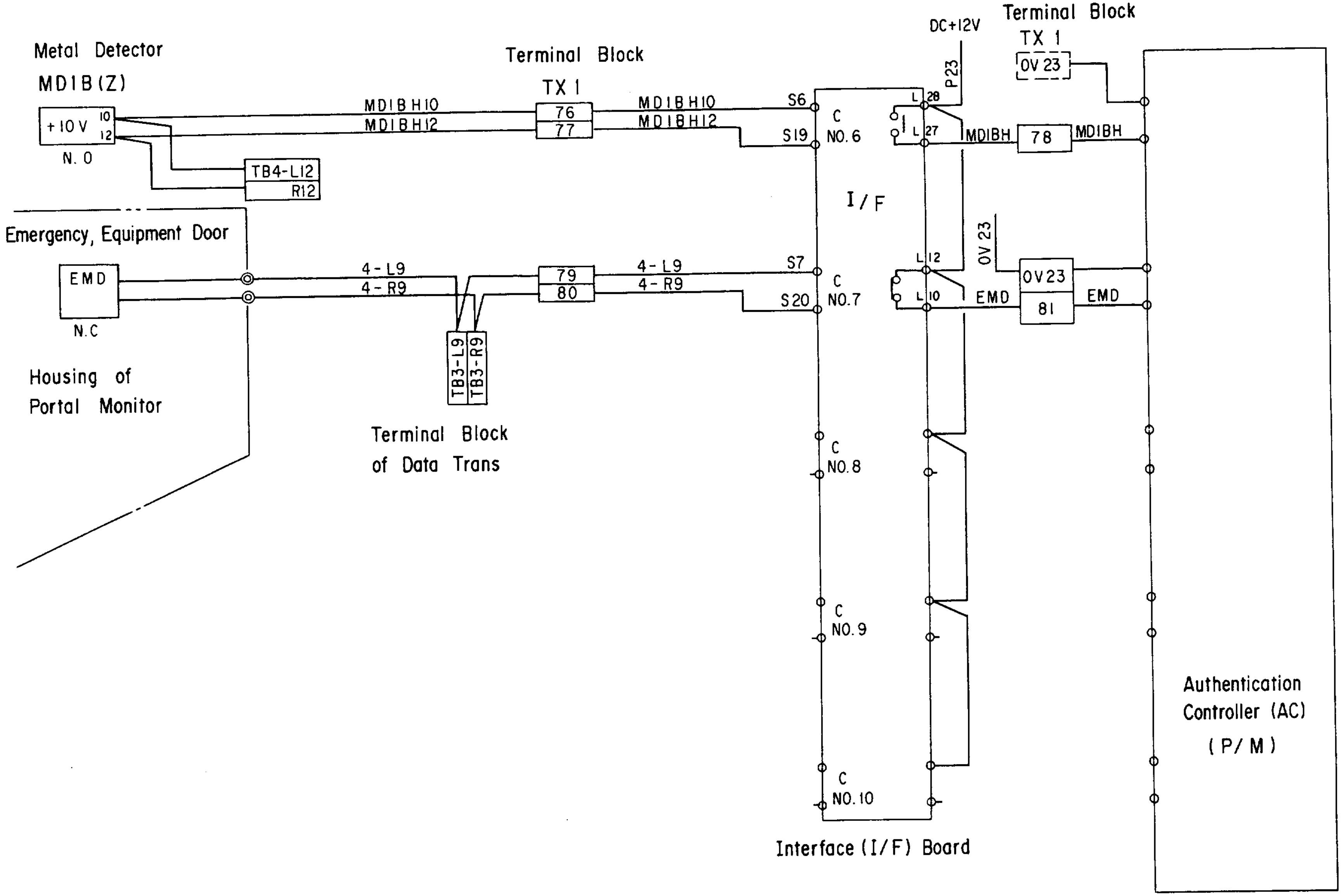


Fig. 23 Sensor Signals for Authentication Controller (AC of P/M) (6/6)

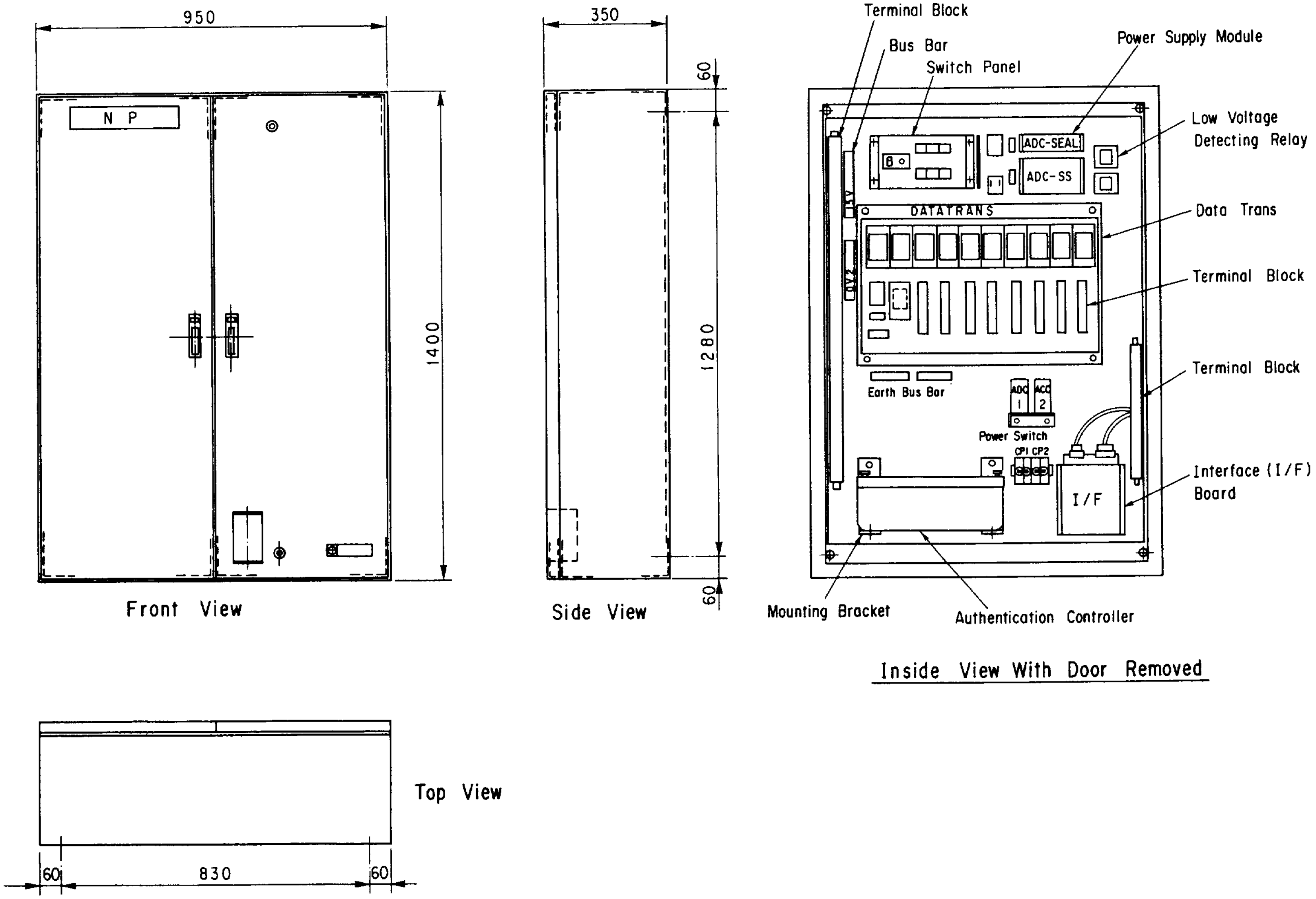
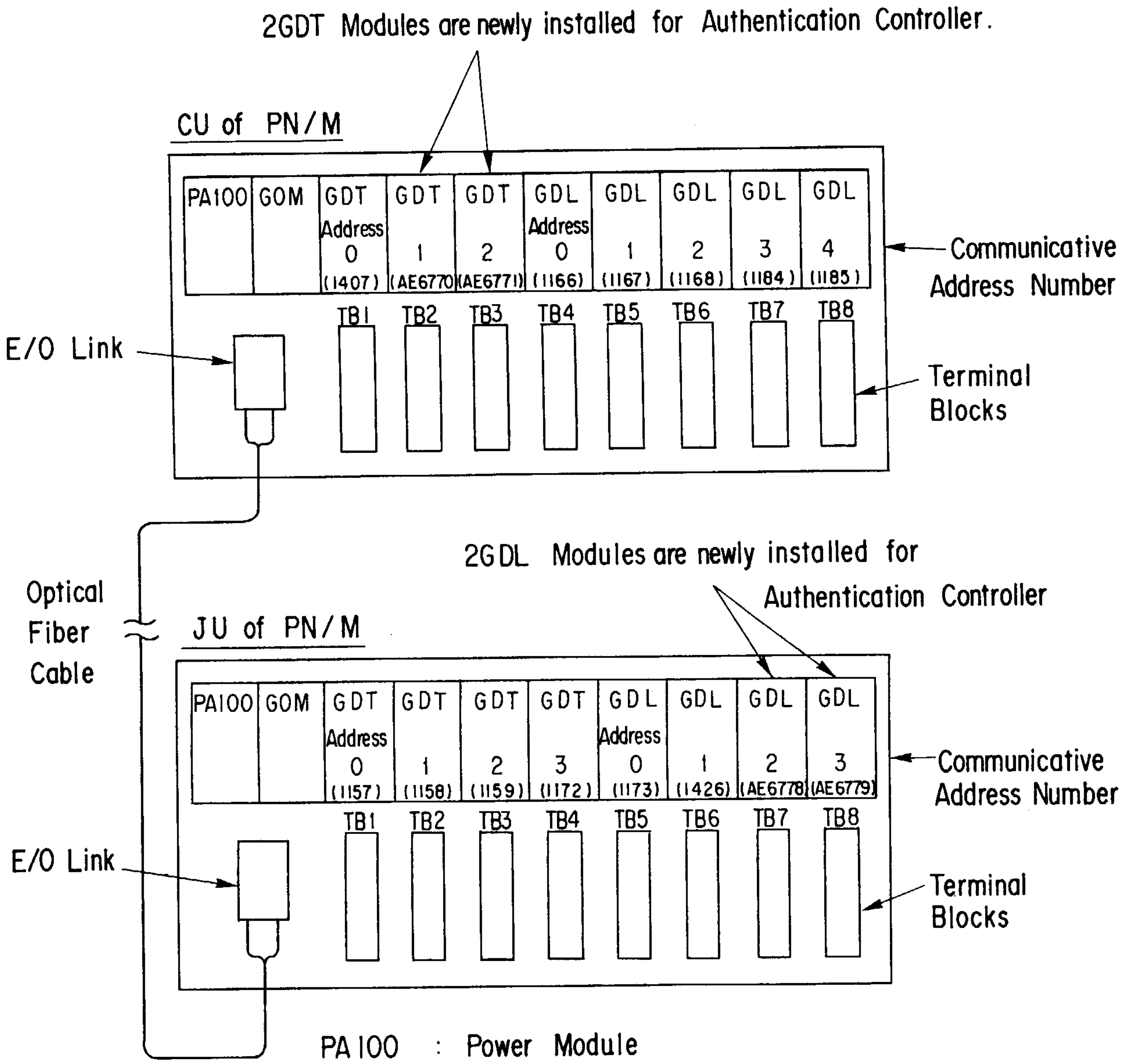


Fig. 24 Junction Unit (JU) of Penetration Monitor (PN/M)


2GDT Modules are newly installed for Authentication Controller.
CU of PN/M
Communicative Address Number
E/O Link
TB1
TB2
TB3
TB4
TB5
TB6
TB7
TB8
Terminal Blocks
Optical Fiber Cable
2GDL Modules are newly installed for Authentication Controller
JU of PN/M
Communicative Address Number
E/O Link
TB1
TB2
TB3
TB4
TB5
TB6
TB7
TB8
Terminal Blocks

CU of PN/M

PA100	GOM	GDT Address 0 (1407)	GDT 1 (AE6770	GDT 2 (AE6771)	GDL Address 0 (1166)	GDL 1 (1167)	GDL 2 (1168)	GDL 3 (1184)	GDL 4 (1185)

JU of PN/M

PA100	GOM	GDT Address 0 (1157)	GDT 1 (1158)	GDT 2 (1159)	GDT 3 (1172)	GDL Address 0 (1173)	GDL 1 (1426)	GDL 2 (AE6778)	GDL 3 (AE6779)

PA100	:	Power Module
GOM	:	Modem Module
GDT	:	Talker (Output) Module
GDL	:	Listener (Input) Module
CU	:	Control and Recording Unit
JU	:	Junction Unit
PN/M	:	Penetration Monitor

Fig. 25 Multiplex Transmitter Devices of Both CU and JU of PN/M

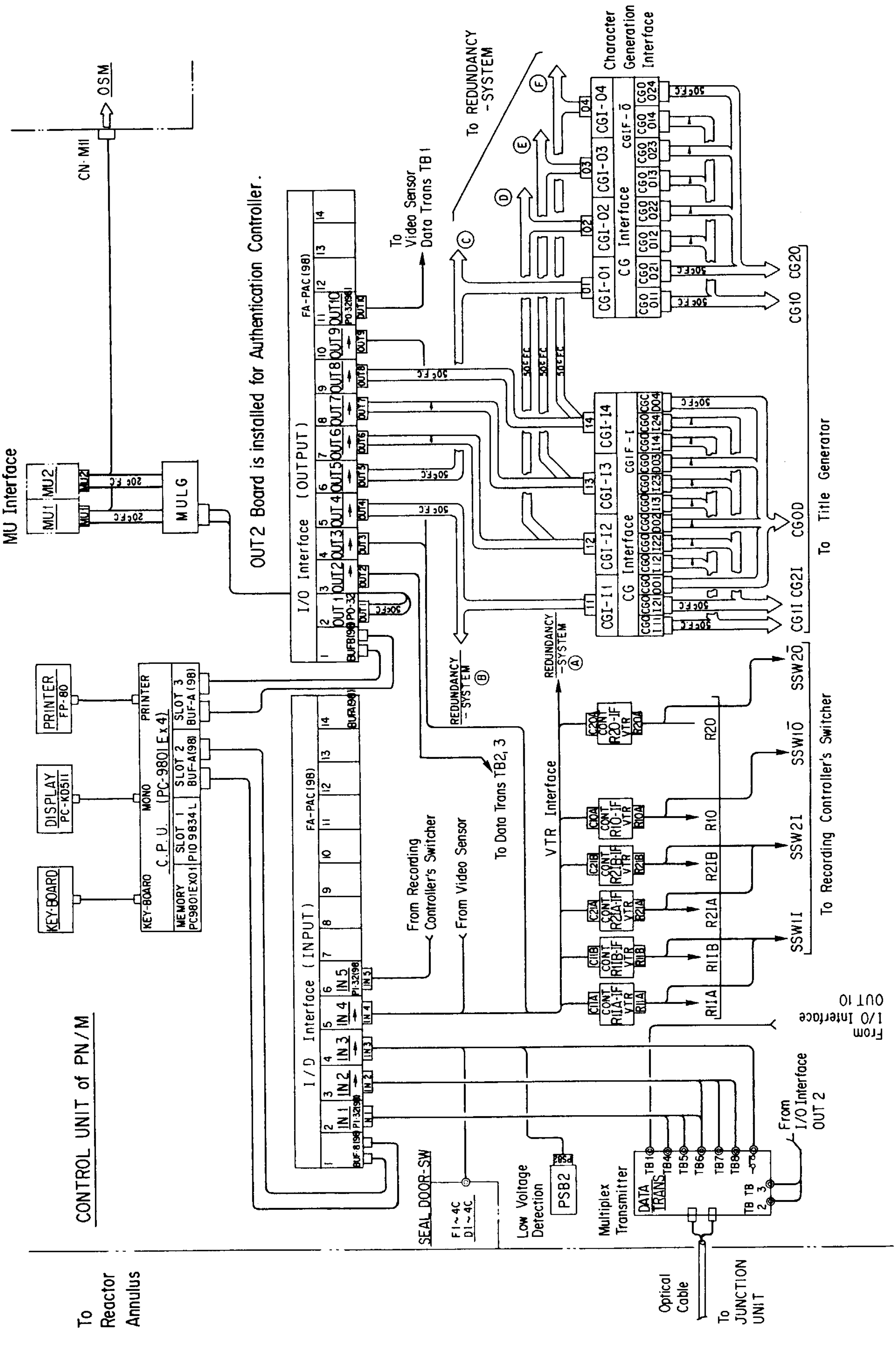


Fig. 26 Wiring Diagram of Control Unit (CU of PN/M)

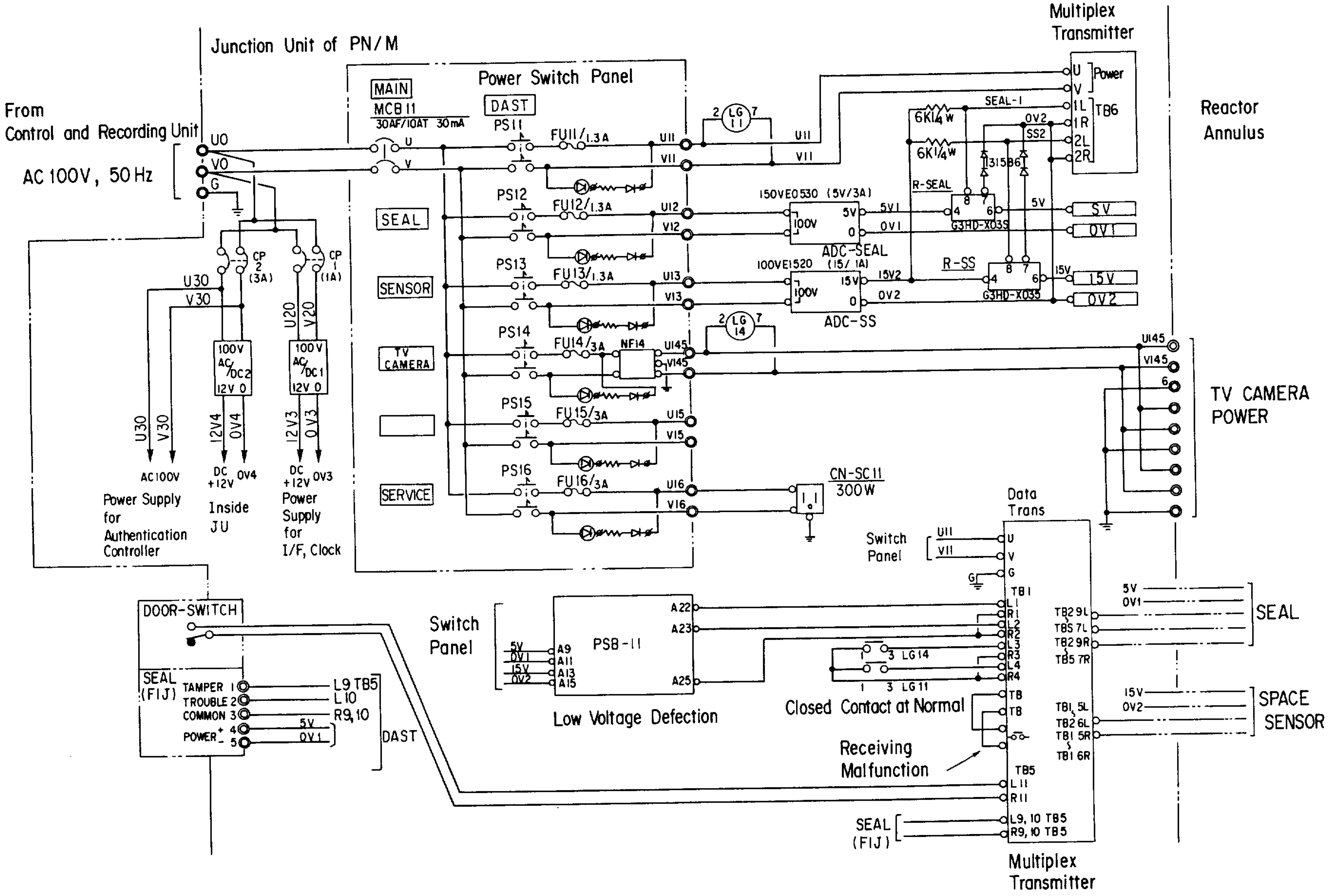


Fig. 27 Power Supply of Junction Unit (JU of PN/M)

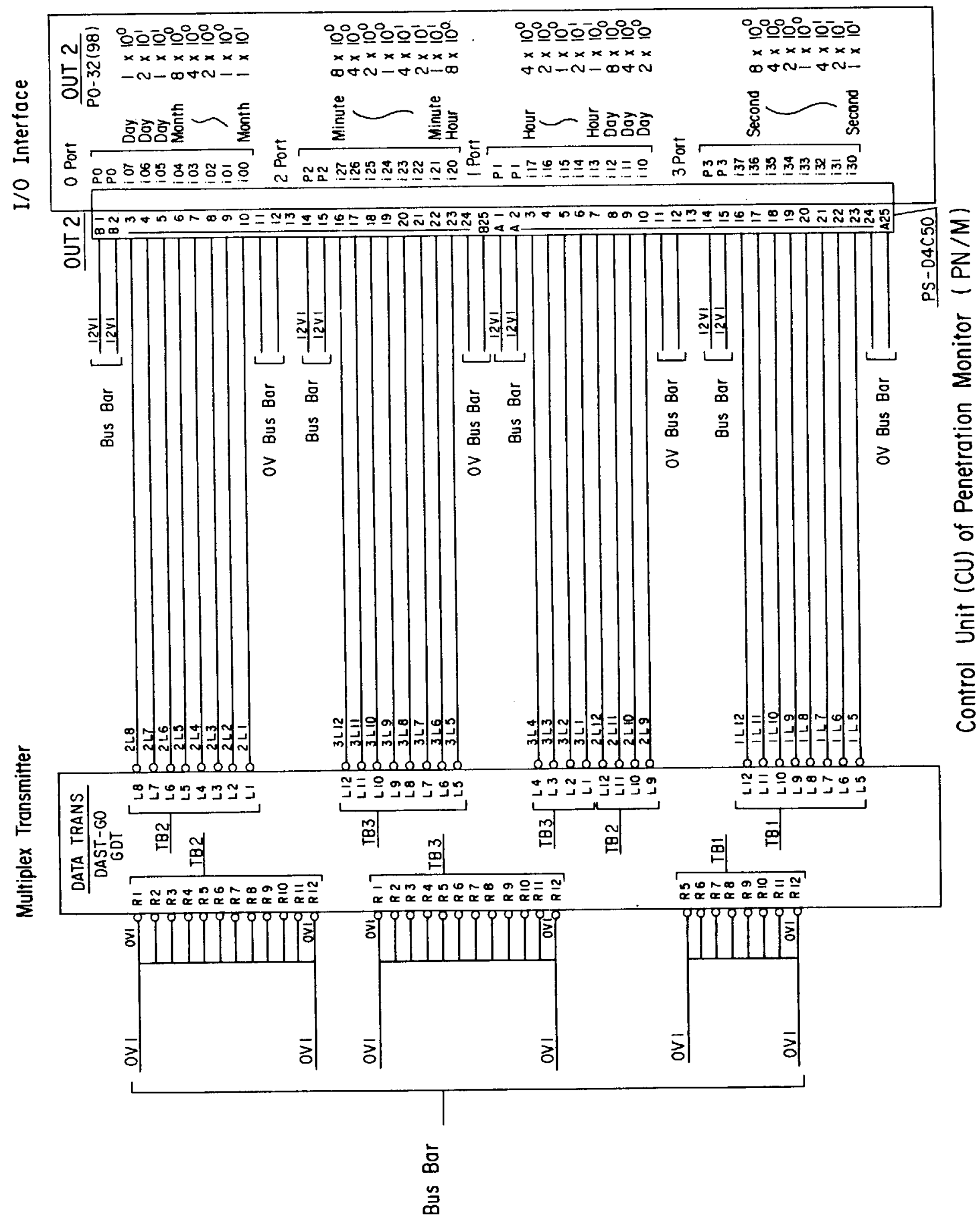


Fig. 28 Clock Signals for Authentication Controller (AC of PN/M) (1/3)

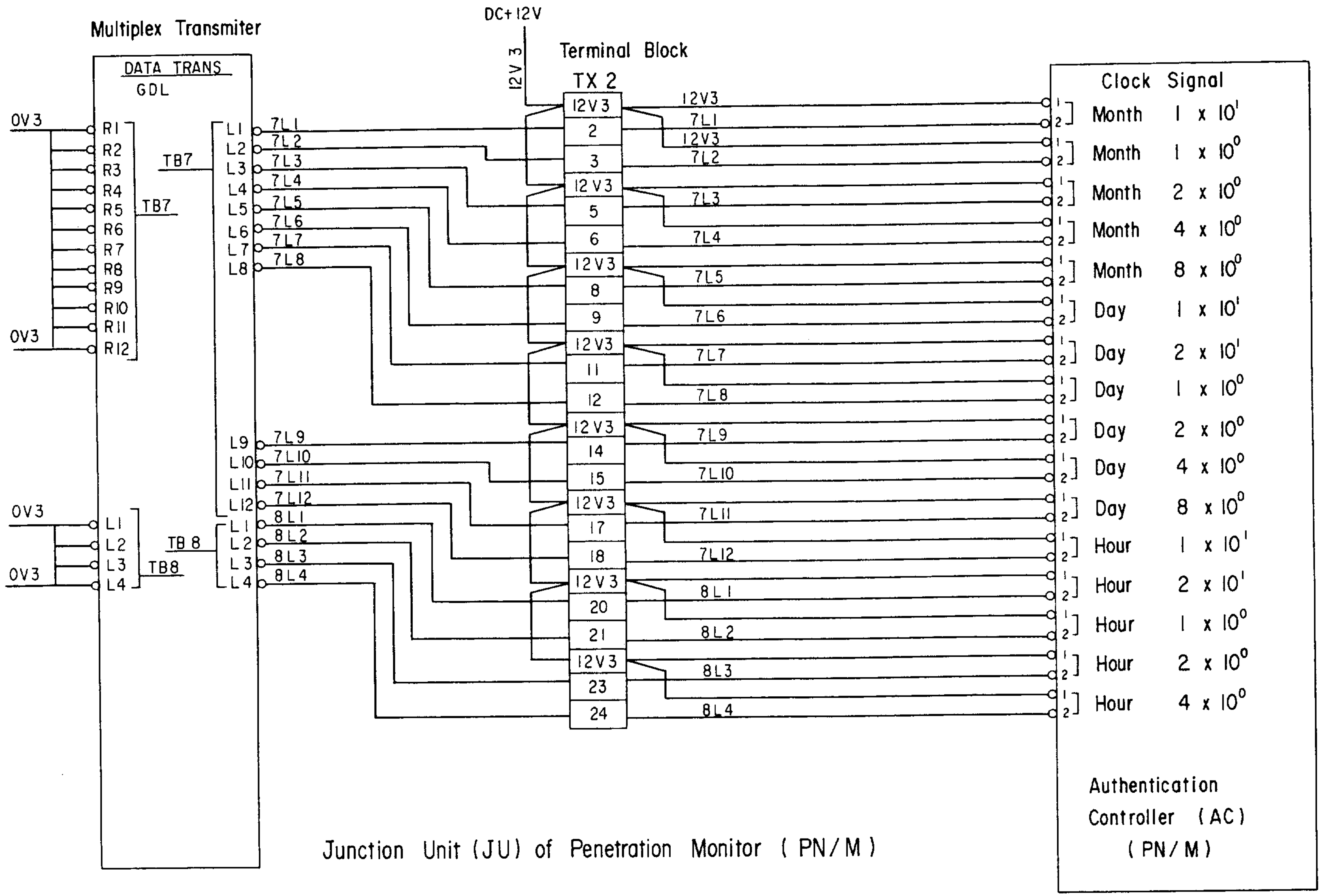


Fig. 29 Clock Signals for Authentication Controller (AC of PN/M) (2/3)

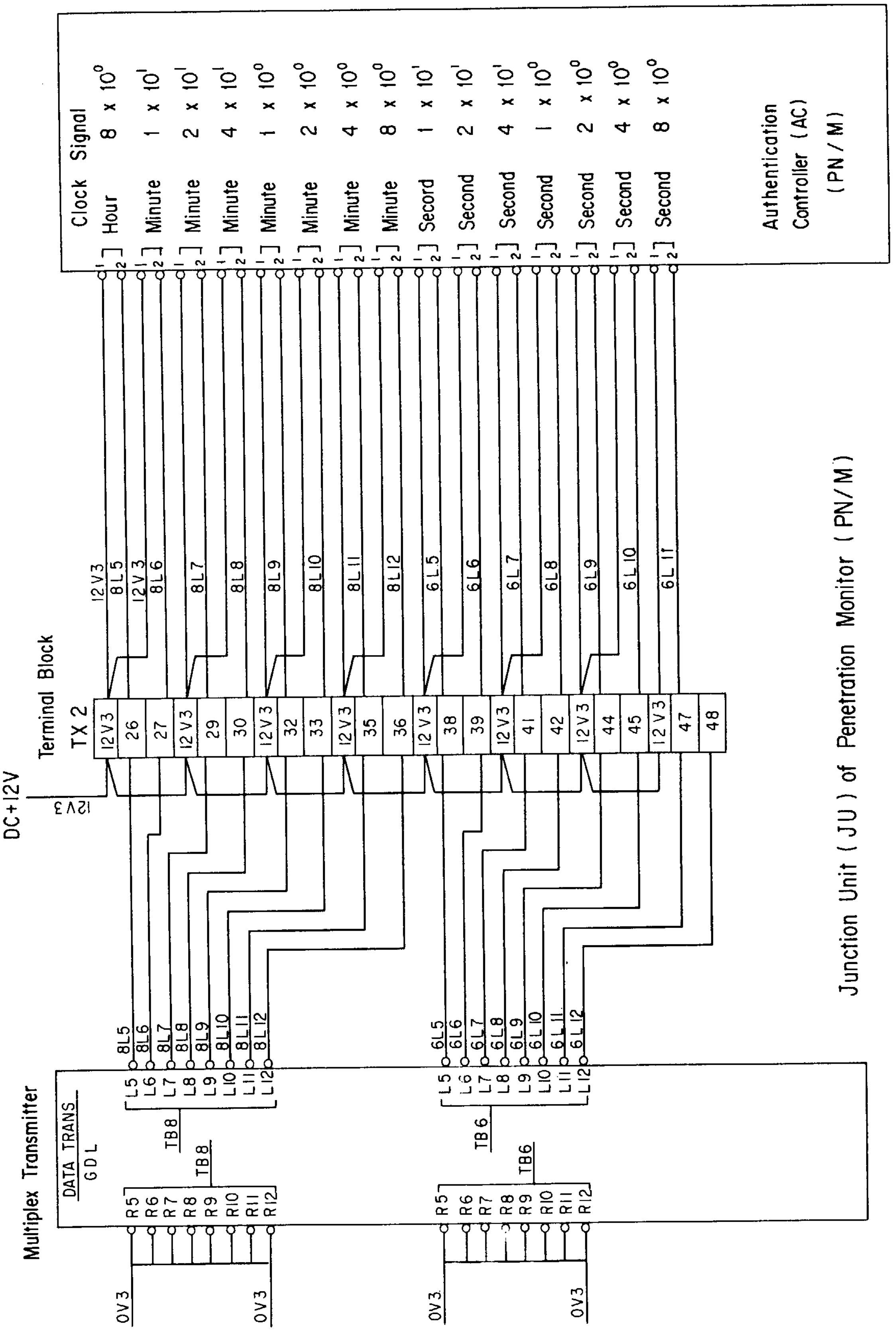

Clock Signal
Hour 8 x 10^0
Minute 1 x 10^1
Minute 2 x 10^1
Minute 4 x 10^1
Minute 1 x 10^0
Minute 2 x 10^0
Minute 4 x 10^0
Minute 8 x 10^0
Second 1 x 10^1
Second 2 x 10^1
Second 4 x 10^1
Second 1 x 10^0
Second 2 x 10^0
Second 4 x 10^0
Second 8 x 10^0
Authentication Controller (AC) (PN/M)
Terminal Block
TX 2
DC+12V
12V3
12V3 26 27 12V3 29 30 12V3 32 33 12V3 35 36 12V3 38 39 12V3 41 42 12V3 44 45 12V3 47 48
12V3 8L5 12V3 8L6 8L7 8L8 8L9 8L10 8L11 8L12 6L5 6L6 6L7 6L8 6L9 6L10 6L11
Multiplex Transmitter
DATA TRANS
GDL
TB8
TB6
8L5 8L6 8L7 8L8 8L9 8L10 8L11 8L12
6L5 6L6 6L7 6L8 6L9 6L10 6L11 6L12
L5 L6 L7 L8 L9 L10 L11 L12
R5 R6 R7 R8 R9 R10 R11 R12
0V3
Junction Unit (JU) of Penetration Monitor (PN/M)

Fig. 30 Clock Signals for Authentication Controller (AC of PN/M) (3/3)

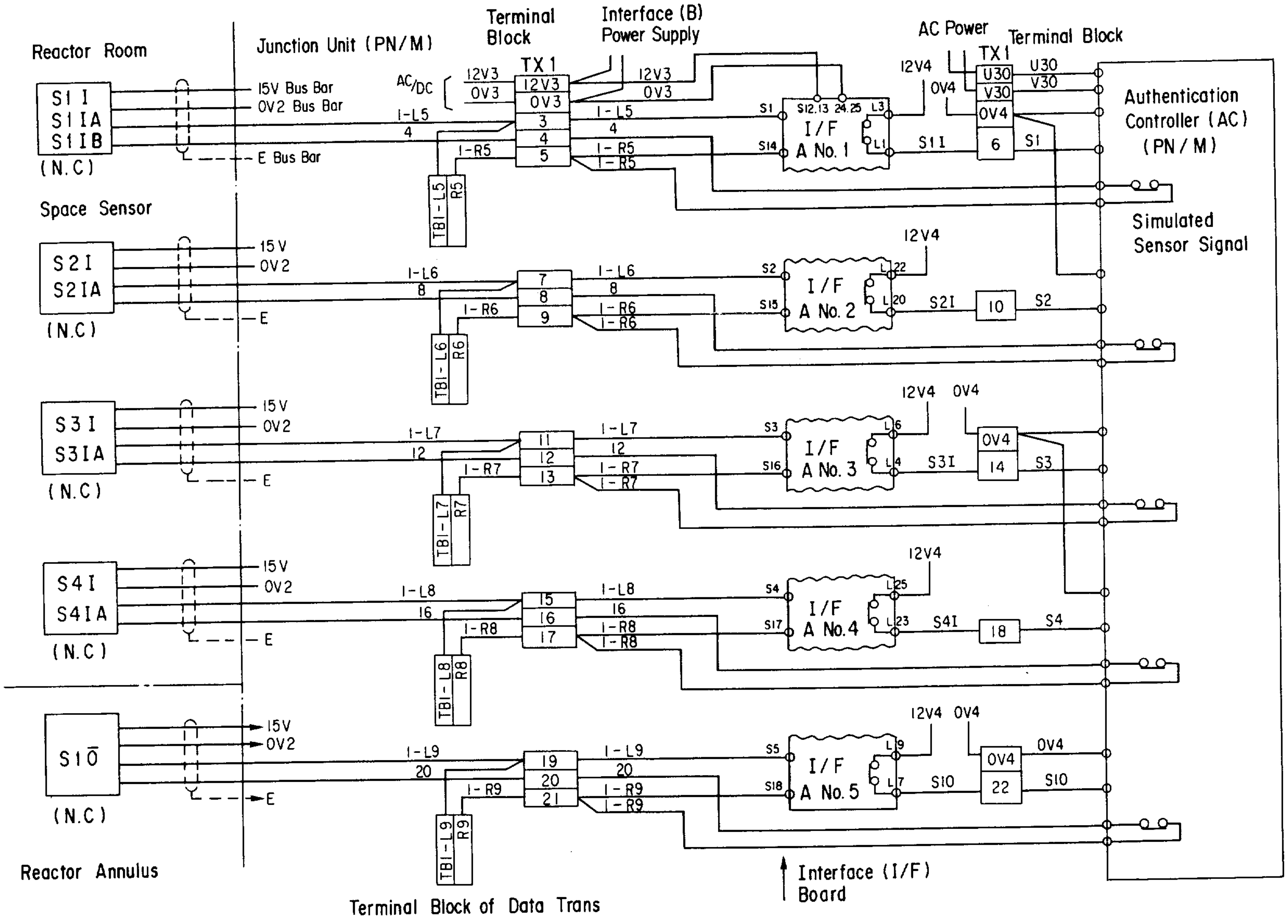


Fig. 31 Sensor Signals for Authentication Controller (AC of PN/M) (1/3)

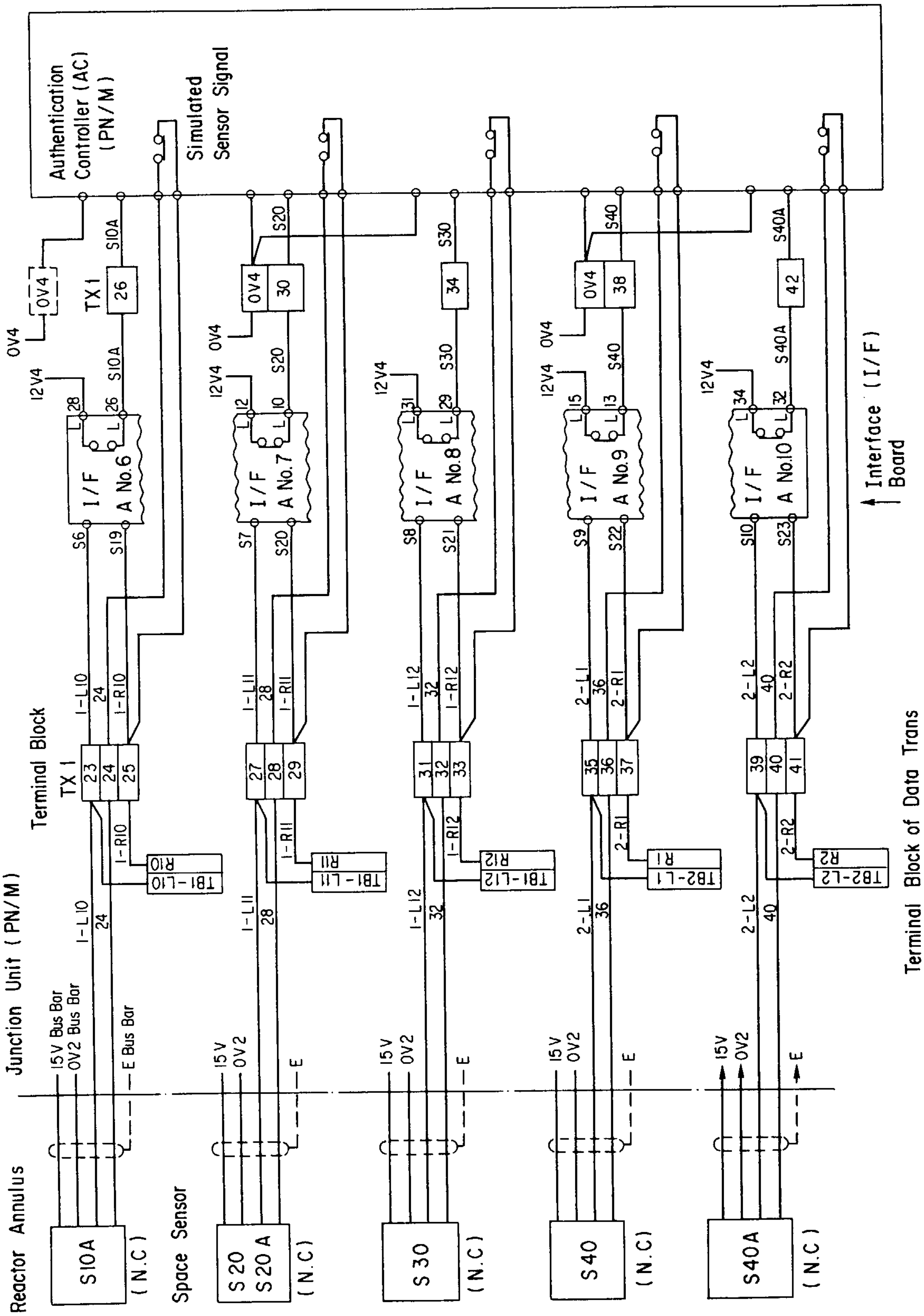


Fig. 32 Sensor Signals for Authentication Controller (AC of PN/M) (2/3)

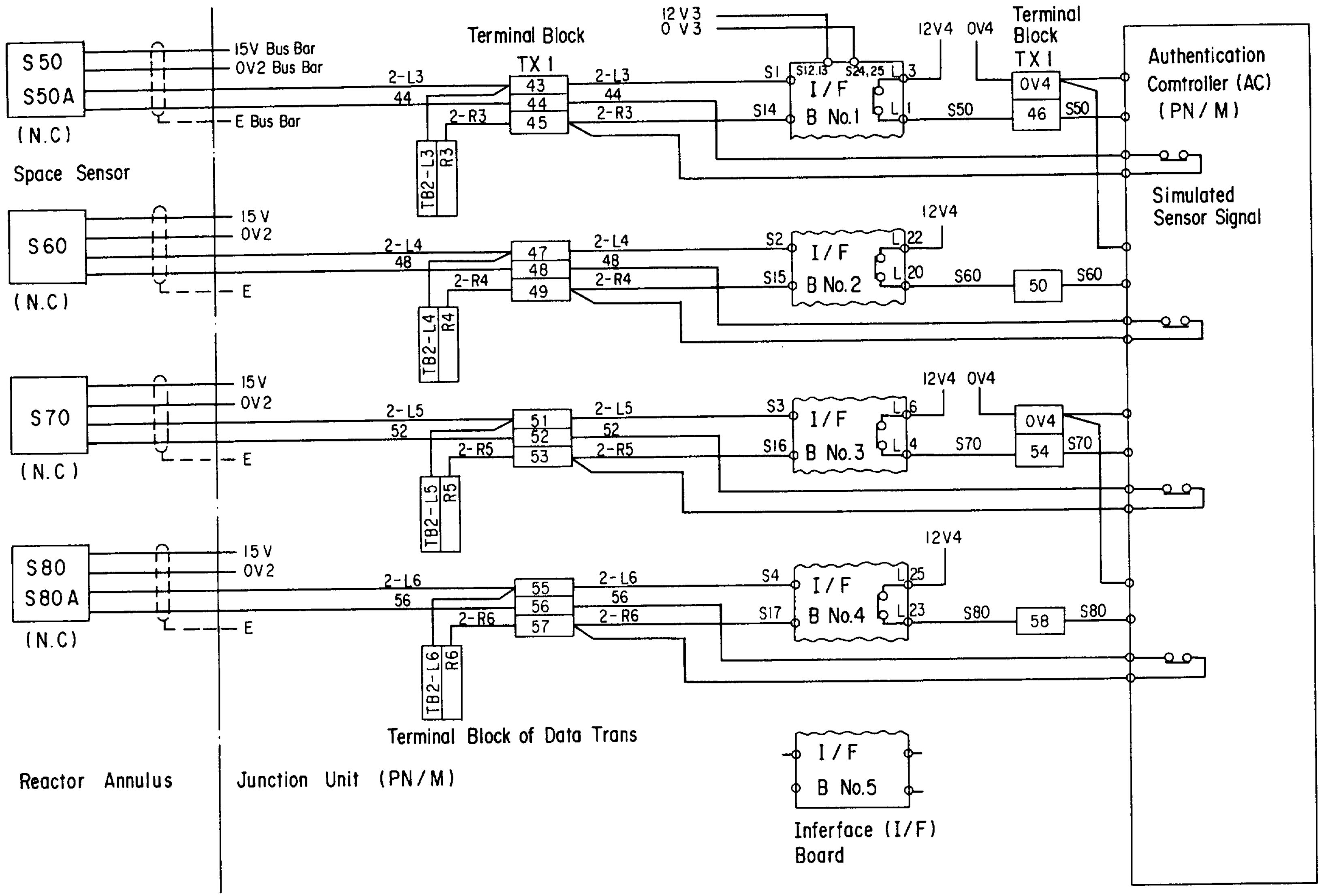
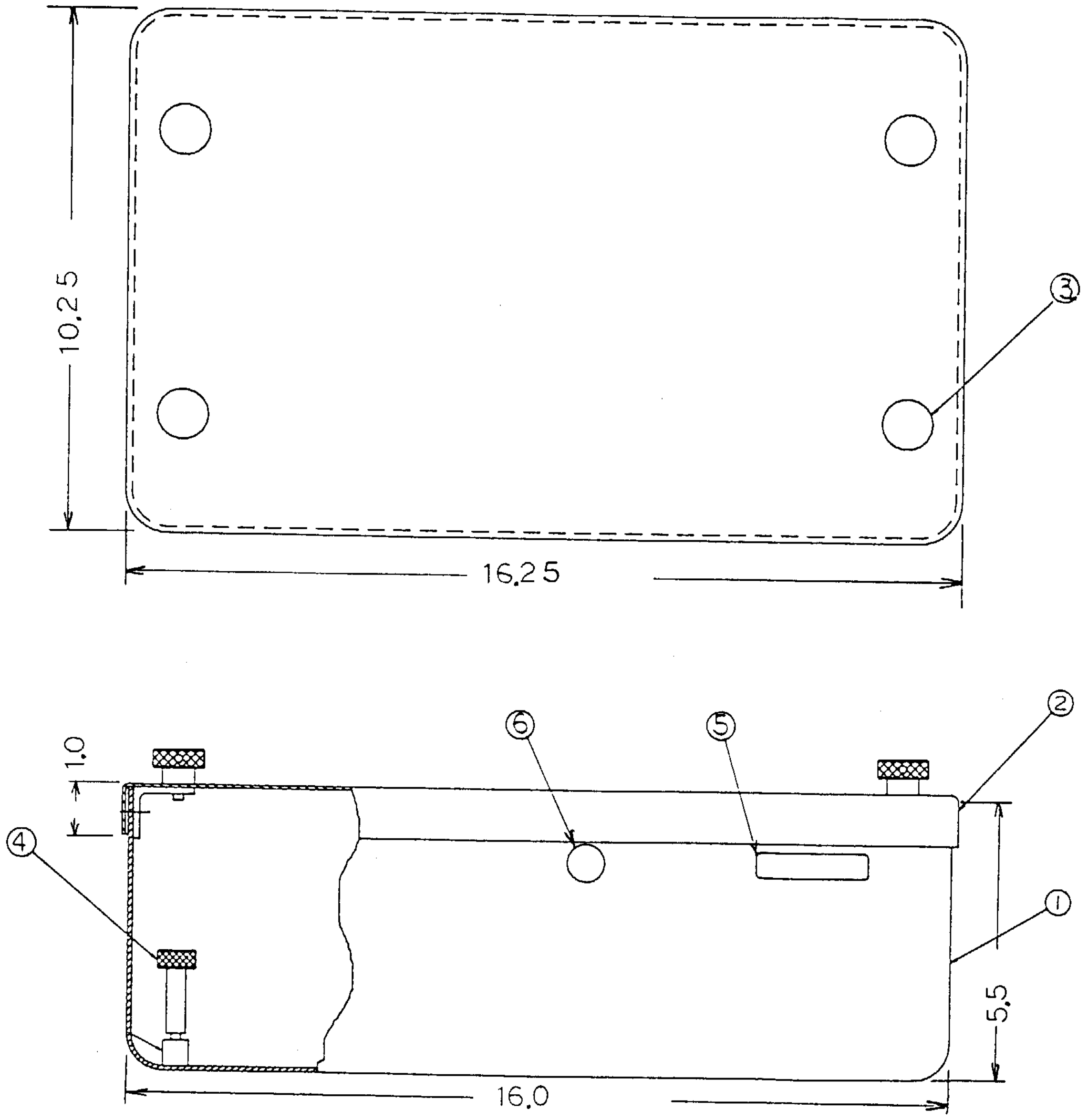


Fig. 33 Sensor Signals for Authentication Controller (AC of PN/M) (3/3)



UNIT : Inch

① Box (Anodized Aluminum)

② Cover (Anodized Aluminum)

③ Thumb-Screw (External)

④ Thumb-Screw (Internal)

⑤ Connector for RS232 Communication

⑥ DataKey Socket

Fig. 34 Housing of the Authentication Controller

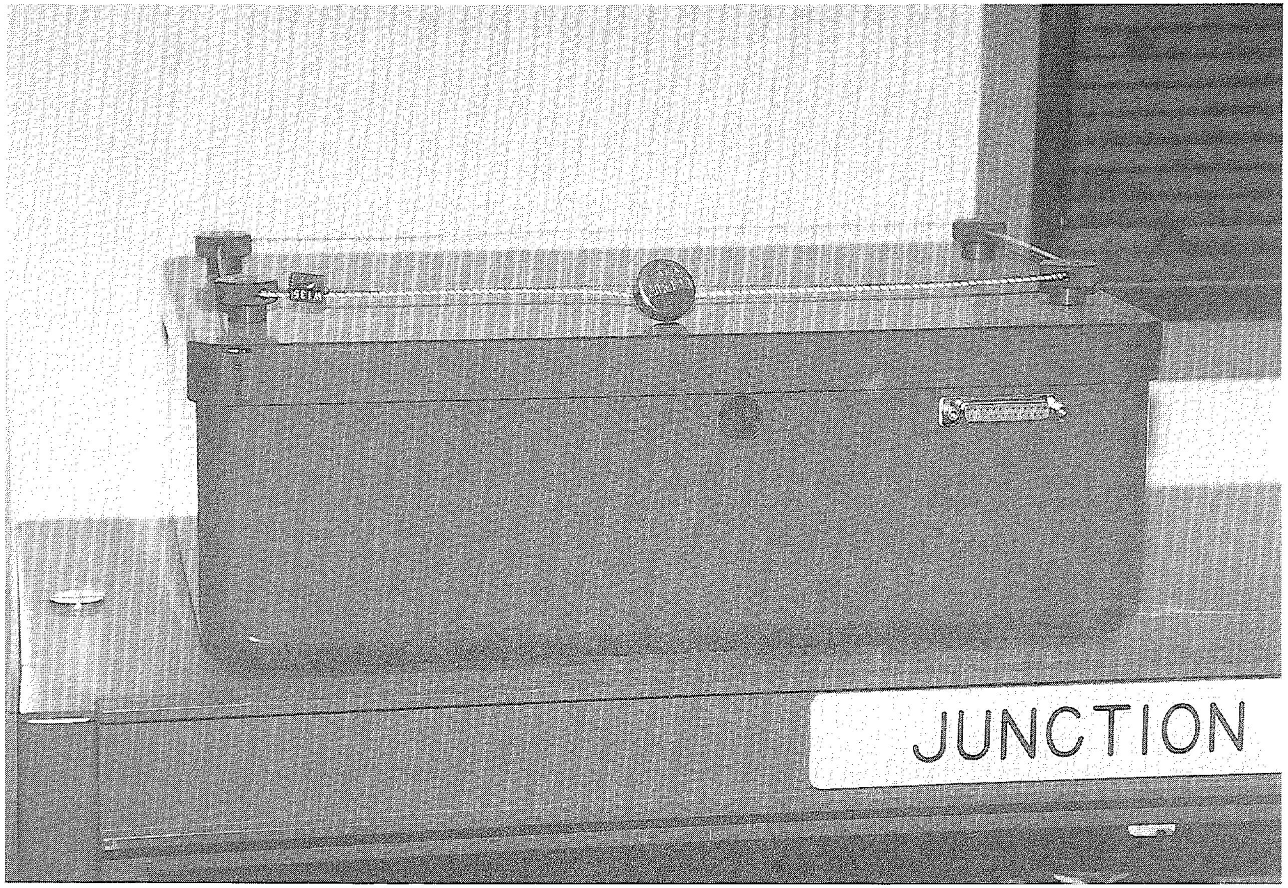


Photo 1 P/M Authentication Controller (AC) with Both Authorities' Seals

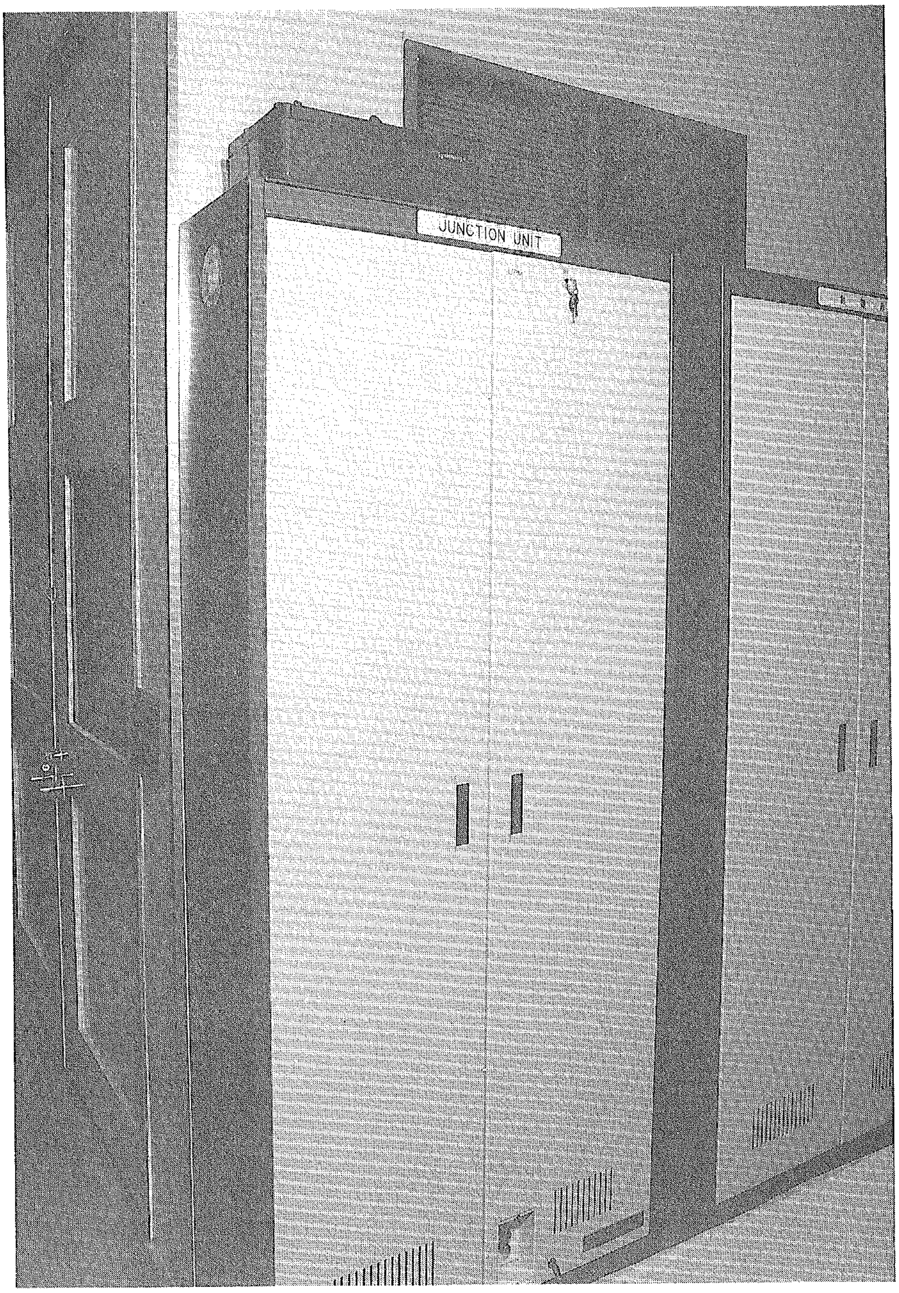


Photo 2 Authentication Controller (AC) on the Top of Junction Unit (JU) of P/M

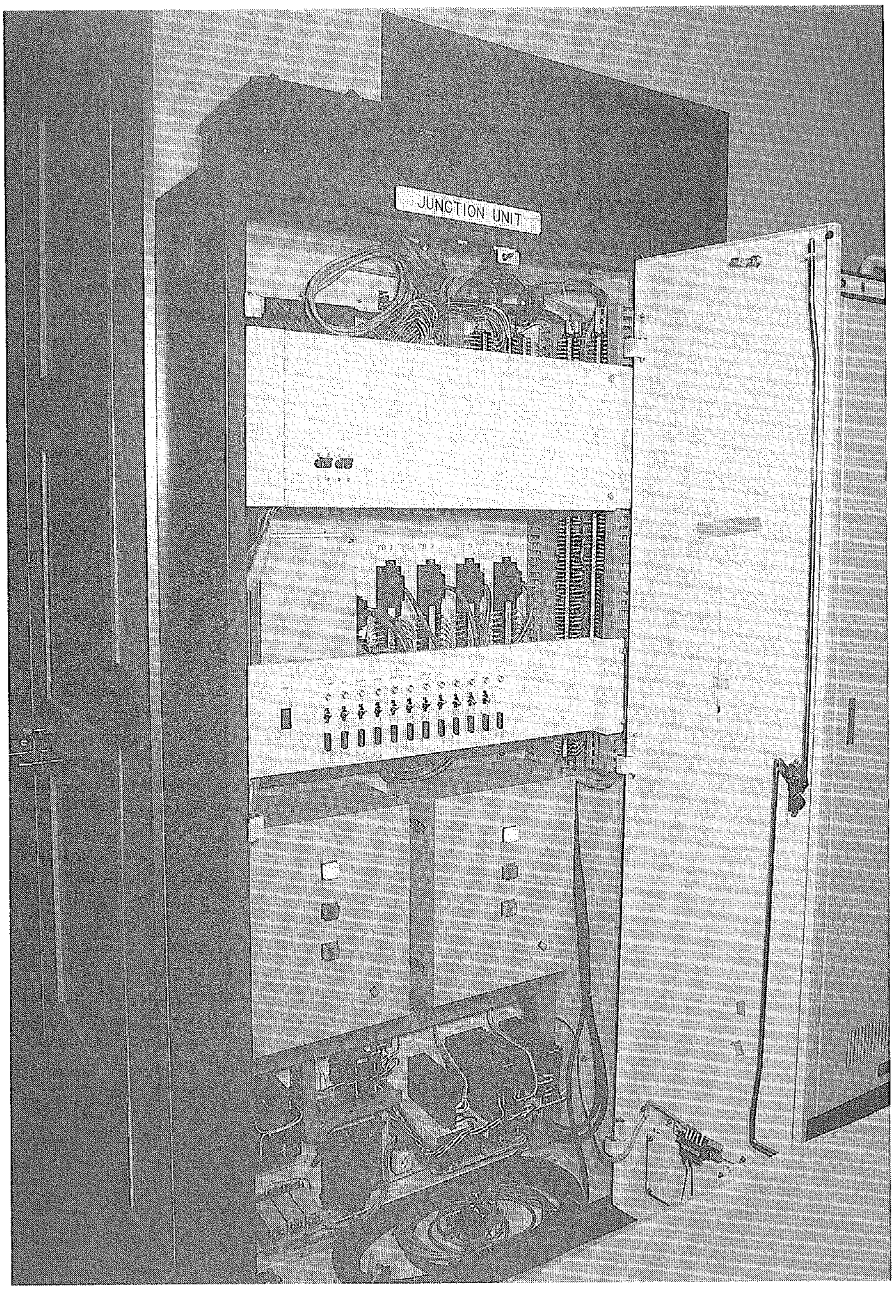


Photo 3 Junction Unit (JU) with Door Removed/Opened and Authentication Controller (AC) of P/M

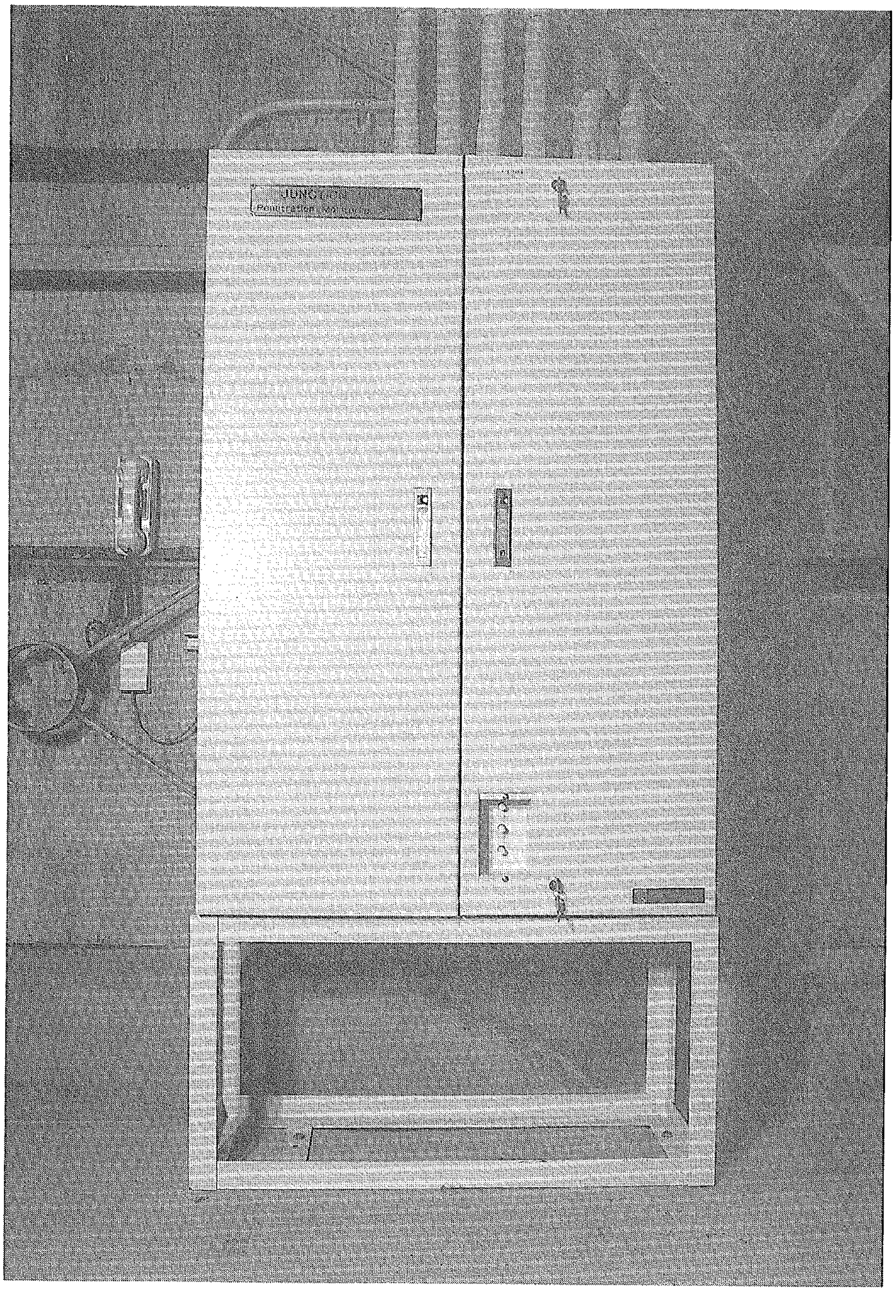


Photo 4 Junction Unit (JU) of Penetration Monitor (PN/M)

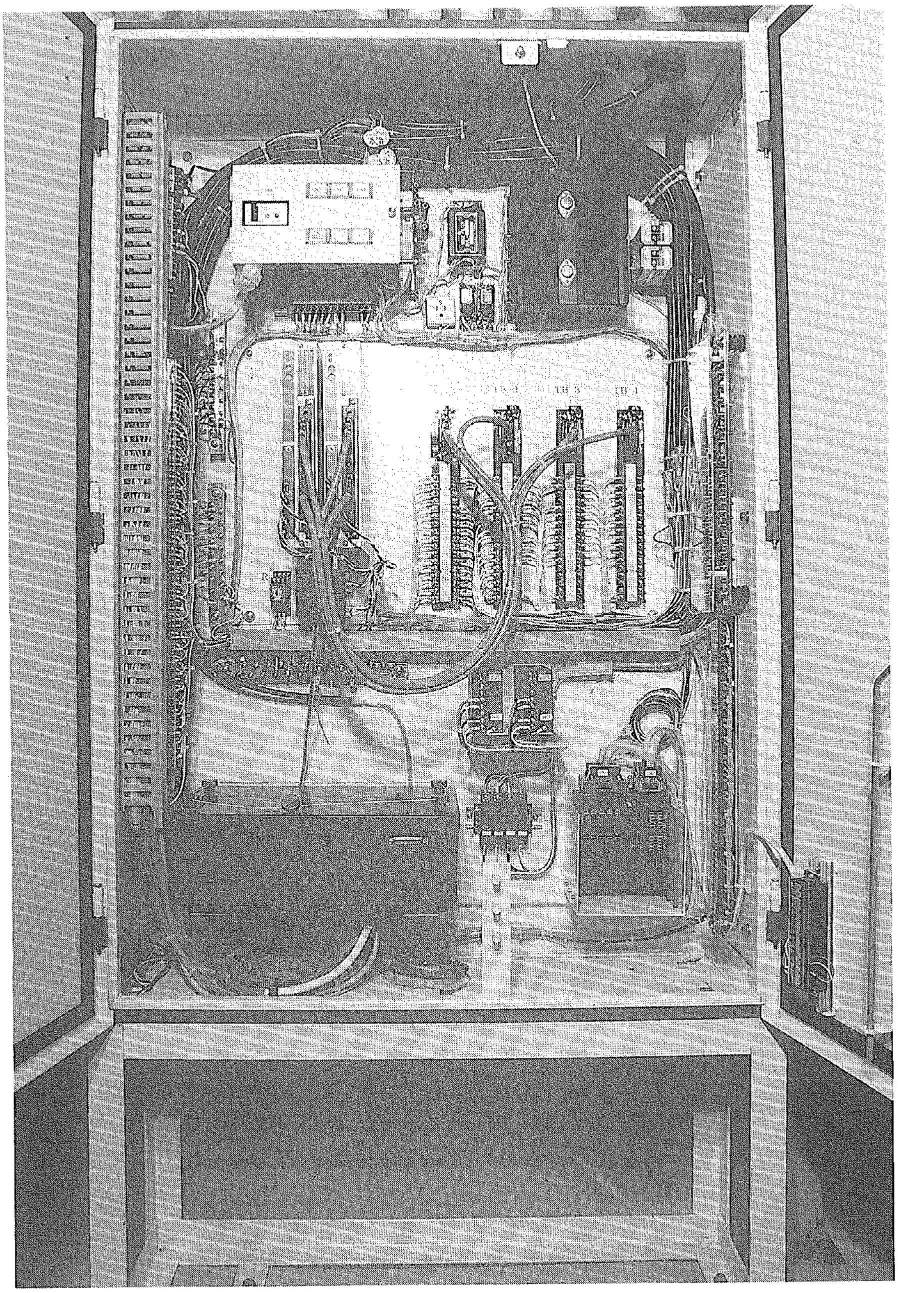


Photo 5 Authentication Controller (AC) inside Junction Unit (JU) of PN /M

Appendixes

1) FCA Authentication Project
   Final Report
   Kenneth j. Ystesund
   On Site Monitoring Technology Department
   Sandia National Laboratories
   January, 1993

2) FCA Authentication System
   Operator's Manual
   Sandia National Laboratories
   November, 1992

3) FCA Authentication System
   Automatic Comparator Manual
   Sandia National Laboratories
   November, 1992

4) FCA Authentication System
   DataKey Operations Manual
   Sandia National Laboratories
   November, 1992

5) FCA Authentication System
   Technical Manual (including drawings)
   Sandia national Laboratories
   November, 1992

This is a blank page.

FCA AUTHENTICATION PROJECT

FINAL REPORT

Kenneth j. Ystesund
On Site Monitoring Technology Department
Sandia National Laboratories
January,1993

FCA Authentication Project
Final Report

Introduction

The Japan Atomic Energy Research Institute designed and constructed an Advanced Containment and Surveillance System for use at the Fast Critical Assembly facility at Tokai, Japan. The AC/S System was built in cooperation with the International Atomic Energy Agency and consists of a Portal Monitor (P/M) and Penetration Monitor (PN/M). Although the AC/S system design has been well documented, the IAEA requires an independent means of authenticating the data recorded by the operator-provided AC/S system. The authentication concept and design requirements of the authentication system were developed by the IAEA and documented by Mr. L. Watkins, IAEA. Sandia National Laboratories (SNL) was given the task of providing a means to authenticate the AC/S system in two phase. Phase I , which was completed with the installation of the authentication system in November 1991, provides the IAEA with the capability to produce reports of sensor activity that must be manually compared to the AC/S system printout. Phase II which was completed in December 1992,permits the automatic comparison of the authentication data to the AC/S data using the personal computer.

Project Funding Support

Design and development of the authentication equipment were funded jointly through the U.S. Program for Technical Assistance to IAEA Safeguards (POTAS) and the Japan Atomic Energy Research Institute (JAERI). POTAS funded the development of the authentication design. The design was presented at a Design Review meeting held at Sandia National Laboratories (SNL) in May 1990. The meeting was attended by the IAEA, JAERI, and SNL. With the approval of the authentication system design by the project participants, the POTAS portion of the project was completed.

JAERI funded the development of the Phase I and Phase II hardware and software, and the installation of the authentication system at the FCA facility in Tokai, Japan.
Authentication Controllers were delivered to the FCA facility in November 1991 and installed. At the same time DataKey hardware was delivered to the IAEA Tokyo

Regional Office (TRO) for use by IAEA inspectors. Software was provided to permit inspectors to program DataKeys at the TRO and to communicate with the Authentication Controllers through personal computers already being used by the IAEA. Also funded by JAERI were the delivery and installation of automatic comparator software that allows the authentication data record to be compared to the data recorded by the FCA Containment and Surveillance Monitoring System. This installation took place during the period Nov.30 – Dec.5, 1992. During that installation complete manuals for the authentication equipment were provided to the IAEA and to JAERI. Table 1 lists the equipment and software provided by funding from JAERI.

Project Background

The Japan Atomic Energy Research Institute started work on the Portal Monitor at the FCA facility in 1979. Construction and testing of the Portal Monitor (P/M) and Penetration Monitor (PN/M) continued until the IAEA issued a final report on the IAEA field trial in February 1990. In 1987 SNL began investigating methods of authenticating the metal detector which is a critical component of the Portal Monitor. This was done to assist the IAEA in determining how to obtain independent authentication of the data produced by the P/M and PN/M equipment. In October 1988 the IAEA documented the requirements for authentication equipment to be installed at the P/M and PN/M. SNL developed a detailed design during 1989 and in May 1990 a design review meeting was held at SNL with participants from the IAEA, JAERI, and SNL. The SNL design was approved by all participants. A tow phase installation of the authentication equipment was completed in December 1992. Table 2 lists documents relevant to the authentication system development.

Equipment Status

When SNL delivered the automatic comparator software in December 1992, changes to the Authentication Controller firmware were implemented based upon results obtained from testing the Phase I system. One of changes to the P/M Authentication Controller was to decrease the relay holding time to 100 – 200 msec when a metal detector self test is initiated. SNL made this change in order to conform to a design specification based upon information provided by L. Watkins, IAEA, in a memo dated 89-02-03. The specification is described in section 3.2 of the SNL Design Specifications document dated May 11,1990. The relay holding time proved to be too short and caused the automatic comparator to incorrectly report metal detector failures. The relay holding time was restored to its original value and subsequent testing done during the December 1992 installation confirmed that the metal detector test results were reported correctly.

Two components of the Authentication Controllers, the nonvolatile memory (NOVRAM) cartridge and the backup battery, should be replaced in 1994. These components were purchased in 1989 and both have a minimum life expectancy of five years.

SNL has identified two software corrections that should be made to the authentication system prior to the year 2000. These do not appear to be serious problems, but should be corrected at the first convenient opportunity. SNL will make the appropriate software changes and keep EPROMs available for installation, or send the EPROMs to the IAEA for installation if that is the preferred method of delivery.

Conclusion

This report concludes the FCA Authentication Project conducted at Sandia National Laboratories. Two Authentication Controllers are in service at Fast Critical Assembly facility in Tokai, Japan. Since the functions of the Authentication Controllers are different, the embedded software associated with each is different. A DataKey interface module is located at the Tokyo Regional Office of the IAEA. This device is connected to an IAEA computer and it allows the IAEA inspectors to program DataKey (potable memory storage devices) which are used to transport Authentication Controller operating parameters from the TRO to the FCA facility. Three software programs, in addition to the embedded software programs, have been provided for use by the IAEA, and each runs on IBM compatible computers provided by the IAEA.

The **Onsite** program permits communication with the Authentication Controllers to program new operating parameters, to start and stop data acquisition, and to download stored data to inspector's computer. **ProgdKey** is the software used at the TRO to program system operating parameters on DataKey memory device.

The **FCAcomp** software is the automatic comparator program that performs comparisons between the authentication data and the data recorded by the P/M and PN/M equipment. Operating manuals and system documentation have been delivered to the IAEA and to JAERI.

Table 1 Equipment and Documentation Provided with JAERI Funding

Equipment or Document	Quant.	Comments
Portal Monitor Authentication Controller	1	
Penetration Monitor Authentication Controller	1	
Loop back connectors (comm. test devices)	2	
Embedded Software for P/M Auth. Controller	1	Version 1.4 delivered Nov. 30, 1992
Embedded Software for PN/M Auth. Controller	1	Version 1.4 Delivered Nov. 30,1992
ONSITE Software (for use by IAEA)	1	Version 2.01 Delivered Dec. 14,1992
DataKey Interface Module with power adapter	1	
DataKeys	8	
DataKey Programming Software	1	Version 1.0 Delivered Nov. 26, 1991
Automatic Comparator Software	3	Version 1.0 Delivered Nov. 30, 1992
Electrical Safety Report (US. Testing Co., Inc.)	1	November 14,1991
FCA Auth. System Operator's Manual	4	November 23,1992
FCA Auth. Sys. Automatic Comparator Manual	4	November 23,1992
FCA Auth. System DataKey Operations Manual	4	November 23,1992
FCA Auth. System Technical Manual	4	November 23,1992

Table 2 Project Documentation

Title	Date	Author
Technical Proposal for FCA P/M and PN/M Authentication Systems	89-02-03	C. Johnson, SNL
Memo to C. Johnson, SNL	89-02-03	L. Watkins, IAEA
Specification of Authentication Equipment for the FCA Portal Monitor(P/M) System – Rev. 2	90-01-29	L. Watkins, IAEA
Specification of Authentication Equipment for the FCA Penetration Monitor (PN/M) – Rev. 1	90-01-29	L. Watkins, IAEA
FCA Authentication System Design Review Meeting - Note to File	90-05-04	IAEA,JAERI, SNL
Design Specifications – FCA Portal Monitor (P/M) and Penetration Monitor (PN/M) Authentication Controllers – Rev. 0	90-05-11	K. Ystesund, SNL
FCA Authentication Controllers Project Quality Assurance Plan	90-11-07	K. Ystesund, SNL
System Test Plan for FCA Authentication Equipment	91-10-15	K. Ystesund, SNL
Electrical safety test report on Authentication Controller design	91-11-14	US. Testing Co.
Pre-installation meeting at FCA facility – draft Note to File	91-08-22	IAEA,JAERI,SNL
Installation of Authentication Equipment at FCA Facility – draft Note to File	91-11-27	SNL
Design Specifications – Automatic Comparator for FCA Authentication Controllers	92-10-20	SNL
Field Test Fast Critical Assembly (FCA) Authentication Equipment	1992	IAEA
FCA Auth. Controller/Comparator Test at FCA JAERI – Note to File	91-12-04	IAEA,JNSB,JAERI ,SNL

FCA AUTHENTICATION SYSTEM

OPERATOR'S MANUAL

Sandia National Laboratories
November, 1992

Table of Contents

FCA Authentication System
Operator's Manual

1. Introduction

The Authentication Controllers installed at the Portal Monitor (P/M) and the Penetration Monitor (PN/M) at the Fast Critical Assembly (FCA) facility provide independent records of sensor activations that occur In the P/M and PN/M. These records are used by International Atomic Energy Agency (IAEA) inspectors to authenticate the records produced by the facility Advanced Containment and Surveillance (AC/S) system. Authentication is accomplished by recording the activations of selected sensors and then comparing this record to the AC/S system record. In addition, the authentication equipment initiates random tests of selected sensors and the expected result is that the sensor activation will be recorded by both the AC/S system and the authentication equipment.

Although the two Authentication Controllers are similar in appearance, there are operational and functional differences because the P/M and PN/M have different functions and require different authentication methods.

This manual describes the operation of the Authentication Controllers and the procedure for producing a report of the data monitored by the authentication equipment.

2. Equipment

2.1 System Description

Overview

Two Authentication Controllers are used at the FCA facility, one at the P/M and another at the PN/M. The P/M Authentication Controller is mounted on top of the P/M junction unit and is accessible without opening the Junction unit or removing a seal. The PN/M Authentication Controller is mounted inside the PN/M junction unit. The controller enclosures can be sealed by routing a seal through the four threaded knobs that secure the cover, however, it is not necessary to remove the cover to operate the equipment. Exterior features of the controllers are a DataKey receptacle and an RS232 port. Communication and programming functions are performed by means of a personal computer and a DataKey through the RS232 port and the DataKey receptacle respectively.

Power Source and Timing

The authentication equipment is microprocessor controlled and normally operates from facility power, but internal batteries will provide a power backup for up to three hours in the event of a facility power loss. Monitored events are stored on a nonvolatile RAM cartridge that will protect the stored data even in the event of a system failure or complete loss of power. Each controller is equipped with a real time clock that is synchronized to the facility AC/S system clock when the authentication equipment is put into surveillance. When an event is recorded, it is tagged with the *facility time* and that time is compared to the internal real time clock. Time differences between the two clocks of greater than two minutes will be recorded as part of the event record.

DataKey Communications

To communicate with the authentication equipment, use a personal computer (PC) that has been loaded with the proper software. If the operating parameters of the authentication equipment must be changed, use a DataKey that has been programmed with the appropriate information. The **Datakey Operations Manual** describes the procedures for programming the DataKey. A DataKey cannot be read by the authentication equipment unless the proper instructions are received from a PC via the controller RS232 port.

Stored Data

Stored data that has been downloaded to a PC is stored on 3.5 inch floppy disks. Report generation software permits an inspector to view and sort the authentication equipment data stored on the disks. The data can then be sent to a printer to produce a hard copy for comparison to the record produced by the facility AC/S system.

2.2 Interface Equipment Requirements

The inspector's computer should meet the following specifications:

- Fully IBM compatible laptop PC with battery backup
- MSDOS 3.3 (or later version) operating system
  (MSDOS FORMAT and LABEL files must be in the system path.)
- 640K RAM minimum

- One IBM compatible RS232 serial communications port (COM 1)
- Centronics compatible parallel port
- One 3.5 inch 720 KB or 1.44 MB disk drive
- A hard disk or RAM drive with 2 MB free for use by the On-Site Services software

See Section 4.3, Cautions, for additional information about the computer equipment and software configurations.

Programming Controllers

Programming the Authentication Controllers requires the use of a DataKey. Procedures for preparing a DataKey are given in the **DataKey Operations Manual**. Operating parameters for both controllers can be stored on a single DataKey.

Data Diskettes

When data is downloaded from the Authentication Controllers to the Inspector's computer, the data is stored on floppy disks. One 720 KB or 1.44 MB data diskette is required for each controller.

RS232 Cable

An RS232 serial communications cable must be used to connect the COM 1 port of the computer to the RS232 port on the Authentication Controller. The cable should be approximately three meters long and one end should mate with COM 1 of the computer. The other end should be a DB-25P connector or equivalent. This cable should be straight-wired, not a null modem or cross- pinned cable, and provide conductors for pins 2-7 and pin 20 at a minimum.

Printing

To print hard copies of reports, a suitable printer should be connected to the parallel port of the computer. The printer and its communication cable to the computer are not specified and are provided by the user.

2.3 Software

Description

The On-Site Services software is provided on a 720 KB disk and includes the

Report Generation program. The software, which conforms to IFSS guidelines, can be run from the floppy disk or loaded onto the computer hard disk. On-Site Services is a menu-driven program which guides the user through the steps to program the authentication equipment operating parameters, start an acquisition period, stop acquisition, and download data to the inspector's PC. These are not the only functions provided by On-Site Services and a more detailed discussion is provided in Section 3.

Disk Space Requirements

The Report Generation program lets an inspector view the data collected during an inspection period, sort that data, and output the sorted data to a printer. During this process the software creates a temporary directory on the computer hard disk and when the program is terminated, the directory is erased and removed. The disk space required for the temporary directory is approximately 2 MB.

Internal Security

When communication is initiated between the authentication equipment and the inspector's PC, the On-Site Services software recognizes which of the two controllers it is communicating with. Similarly, the Authentication Controllers respond only to a computer using an authorized version of the On-Site Services software because each message contains embedded passwords are not displayed on the computer monitor. Repeated attempts to communicate with an Authentication Controller without the proper software causes the controller to lock out its RS232 port for one hour.

Limitations

As previously stated, a DataKey alone cannot be read by the authentication equipment unless a computer running the On-Site Services software is connected to the controller. The computer used without a properly programmed DataKey cannot change the operating parameters of the authentication equipment, however, the computer will allow a user to start and stop surveillance as well as perform other functions.

Note: To maintain system integrity, it is important to protect the software with its embedded passwords as well as the computer containing the software.

3. Procedures

3.1 Installation and Setup

Floppy Disk Procedure

1. Connect the Authentication Controller RS232 port to the computer COM1 connector before turning on the computer.
2. Turn on the computer.
3. Go to a DOS prompt, for example C:/>,if one is not displaying already.(If you have Windows or a menu system that displays when you turn on the computer, you must exit to DOS completely. Do not use the DOS prompt option from the Windows Program Manager.)
4. Insert the On-Site Service diskette into the appropriate disk drive if the program will be run from the floppy disk. Enter the designation of the selected drive followed by a colon, for example, A:
5. Type the command ONSITE and press ENTER, for example: A:>onsite

Monitor Settings

When this command is entered, the software defaults to either color or monochrome(black and white), depending upon the computer setup. The user can choose to run the program in either color or monochrome by entering the command “onsite color” or “onsite bw”. When ONSITE is run on a laptop computer with an LCD screen, use the “onsite bw” command to improve the contrast.

Running From the Hard Disk

If On-Site Services has been installed on the computer hard disk, type the command ONSITE from the directory containing the software. A “Checking floppy drive...” message appears while the software checks for the existence of a 3.5 inch floppy disk drive. When there is a diskette in the drive (assuming that there is a 3.5 inch drive) the software immediately displays the title screen, but if there is no diskette in the drive a DOS error message may appear on the screen indicating an error reading the drive. (This response depends on the model of computer and its hardware configuration.) The user has several options at this point:

- Insert a diskette into the drive and type R(for Retry) to advance the software to the title screen, or,

- If the user does not wish to insert a data diskette into the disk drive at this time, type R(for Retry), or A(for Abort) to bring up the title screen. Due to differences among computers the keyboard response which causes the program to advance to the title screen may vary, but one or more of the three responses (Abort, Retry, or Fail) will successfully clear this DOS message.

Set Date and Time

The first screen to appear is the title screen and the operator may check or set the current time and date. Pressing the up and down arrows let the user select either date or time. The user may enter correct values. Press the ENTER key to record the changes or confirm the existing values. When the user has entered new values or accepted the current values of the time and date, the software displays the Main Menu. The current time and date appear at the top of the screen.

3.2 General Instructions

Help

User instructions display at the bottom of the screen. For additional help, press F1 at any point in the program to run the Help utility. To choose a menu option, type the first letter of the option, or use the arrow keys to move the cursor to the desired option and press Enter.

3.3 Main Menu Options

Controller Services

This option initiates communication between the computer and the Authentication Controller. Upon selection of this option, the controller identifies the controller (PN/M or P/M) or notifies the user that communication cannot be established. If repeated attempts to establish communication fail, the user returns to DOS automatically. When communication is established and the controller is identified, either the P/M or PN/M Authentication Controller Menu appears. When communication is established with an Authentication Controller that is in acquisition (monitoring and storing data), the acquisition period ends and the current date and time are recorded.

Diskette Services

Diskette Services are utilities that permit the user to check data on a diskette that might be used as a data diskette, and to format diskettes properly for use as data diskettes. Data that is downloaded from the PN/M Authentication Controller must be transferred to a data diskette that has been formatted as a PN/M data diskette. This feature facilitates the identification of data during the report generation process.

Report Generation

The Report Generation option allows the user to select an acquisition record, clock synchronization data, or self test data from a data diskette. The acquisition data can be stored by sensor or time. All data can be reviewed on the computer monitor or printed.

Loop-Back Test

This is a diagnostic feature included as a trouble-shooting aid in the event of a communication problem between the computer and the authentication equipment. If communication cannot be established with an Authentication Controller the problem could be with the controller, the communication cable, or with the computer. If a loop-back connector is plugged into the COM1 port of the computer, the loop-back test checks the I/O functions of the computer. When a loop-back connector is installed at the end of a communications cable that is plugged into COM1, the cable integrity is tested as well as the computer I/O functions. See the trouble-shooting section of this manual for further aid in isolating system problems.

Quit to DOS

Select this option to exit On-Site Services and return control to the computer operating system.

3.4 P/M or PN/M Authentication Controller Menu Options

End Acquisition Period

Choose this option to have the Authentication Controller stop collecting data and record the date and time that acquisition ended. Acquisition records automatically when the user selects Controller Services from the Main Menu, but this option allows the user to end acquisition from the Controller Services Menu if an acquisition period that has just been started must be halted.

Download Acquisition Data to PC

When this option is selected, the software interrogates the controller to determine the file size required and checks that information against the available storage space on the data diskette. If a data diskette has not been inserted into the disk drive, a prompt asks the user to insert a disk. If the inserted diskette has not been properly formatted, a prompt instructs the user to go back to the Diskette Services Menu and prepare a data diskette. After these checks have been made, the software transfers the data stored in the Authentication Controller to the data diskette.

Program Authentication System Parameters

Programming the system parameters requires the use of a DataKey that has new operating parameters stored on it. The authentication equipment cannot be reprogrammed during acquisition so the acquisition period should not be started until the new parameters are read into the Authentication Controller. The computer screen prompts guides the user through the process of programming new operating parameters into the controller.

Start Acquisition Period

This option causes a sequence of events to occur. The authentication equipment synchronizes the on-board clock to the FCA C/S system clock. The appropriate data diskette should be in the disk drive because the clock data is stored at this time. The user is prompted to insert the diskette if it is not in the disk drive. Both clock times are stored before and after synchronization. The reason for storing this data is to help resolve any time difference flags that may have occurred during the previous acquisition period and to verify that synchronization is accomplished at the beginning of the next acquisition period. The clock synchronization data displays on the computer monitor for review by the system user.

When the clocks have been successfully synchronized and the clock data transferred to the data diskette, the authentication equipment begins to monitor and stores data according to the operating parameters most recently loaded into the system.

It is possible to start acquisition without downloading data, however a system prompt asks the user to confirm the request to assure that stored data does not need to be saved. When acquisition starts, the authentication equipment memory is cleared and the stored data is lost unless it has been downloaded. Therefore, if the data from the previous acquisition period must be saved, it should be downloaded to a data diskette before attempting to begin a new acquisition period.

Controller Self Test

Each Authentication Controller has a self test routine that can be run when the controller is not in acquisition. Because the functions provided by the P/M and PN/M authentication equipment are different, the self tests are also different. The approximate time required for each of the two self test procedures is two minutes. Both controllers test the system memory which consists of RAM and a non-volatile memory cartridge (NOVRAM) which is used to store the data during an acquisition period. Results of self tests display on the computer screen, including memory test failures, and are also written to the data diskette to create a record of the self test results. Self test features which are unique to each controller are described below:

P/M Authentication Controller

Since there is no capability to test individual sensors in the P/M, the self test does not activate sensors. The metal detector MD1 can be randomly tested during an acquisition period, but the self test does not provide this capability through software. If a test of the metal detector circuit is required, there are two push-buttons inside the controller enclosure that activate the metal detector self test. The buttons are labeled MD1-A and MD1-B and they actuate the self test circuits in the metal detector if all wiring connections are correct and the metal detector self test circuits are adjusted correctly.

PN/M Authentication Controller

In addition to memory tests, the self test checks the controller's capability to activate individual sensor relays and to read the resulting simulated sensor activation. The first step in this process is to read the “normal" status of each of the PN/M motion detector sensors. Then each sensor relay is sequentially activated and read again. If all sensors check out correctly the computer monitor displays a message that the system passed the self test. If a discrepancy is recorded the user will be informed which sensor failed the test. **This self test should only be performed when the PN/M area is unoccupied** because any sensors that are actuated during the test will appear to be operating incorrectly.

Quit to Main Menu

Choose this menu selection to return to the On-Site Services Main Menu.

3.5 Diskette Services Menu Options

List Files

Before formatting a diskette as a data diskette the user may want to check the contents of a diskette or to determine whether or not an unknown diskette is an FCA data diskette. This option checks the diskette and reports the disk contents to the user. If the diskette has been previously formatted as an FCA data diskette, the screen displays the system for which the diskette has been formatted (P/M or PN/M) and what files, if any, have been stored on the diskette. If the disk has never been formatted, that information displays. When the diskette contains DOS files, the directory displays to allow the user to determine if the files should be saved. When the disk contents display, press the cursor arrow keys and the Page Up and Page Down keys to scroll the directory.

Format a Penetration Data Diskette

Select this option to format a diskette and tag it as a Penetration Monitor data diskette.

Format a Portal Data Diskette

Select this option to format a diskette and tag it as a Portal Monitor data diskette.

Quit to Main Menu

Choose this option to return to the On-Site Services Main Menu.

3.6 Report Generation Menu Options

Choose Drive For Files

When you select Report Generation from the Main Menu, the software prompts you to enter the letter of a disk drive or RAM drive with at least 2 megabytes of available memory space. In most cases, type “C” for drive C, however, an alternative drive can be selected. Next, you must insert a data diskette into a disk drive. (When ONSITE is first started, the software checks for the existence of 3 .5 inch disk drive and records the letter designation of the 3.5 inch drive.) When the system detects a valid data diskette in the disk drive, the Reports Menu displays.

Viewing Data

The data displays in “scrollable regions” which let you use the cursor arrow keys to scroll up, down, and sideways through the data because the data “page” is longer and wider than the data windows.

To print the data presented in the Reports Menu, press the ALT and P keys simultaneously.

To stop a print operation, press the ESC key.

Acquisition Data

When data is downloaded from an Authentication Controller to a data diskette, the acquisition data is stored in a file that is identified according to the date that the acquisition period started and a sequence number. For example, if two acquisition periods were started and stopped on the same day, there would be a MMYYDD01 file and a MMYYDD02 file. Use the cursor arrow keys on the computer keyboard to scan up, down, and sideways through the data. When the file of interest is found, select it by positioning the cursor on the record and pressing the ENTER key.

Report Format

The acquisition data displays in a report from consisting of data entries with seven column of information. The column headings and their meanings are explained below:

- Event -

An event is the designation for a particular sensor or a condition that has been recorded during an acquisition period. In most instances the event is self explanatory, but some event designations are unique to the authentication equipment and do not have a corresponding event in the AC/S system. MD1A5, MD1B5, MD1A10, and MD1B10 are designations for the four metal detector outputs. These events are not directional and only serve to identify the individual outputs. The INCORRECT SB4,5,6 SEQ event refers to an incorrect beam sensor sequence or a time-over condition in the zone monitored by SB4,5 and 6. The sequence must be either 4-5-6 or 6-5-4 within a ten second window, or else an INCORRECT SB4,5,6 SEQ event is recorded. (When this event appears on a printout it is abbreviated to INCORRECT.) The ten second time-over event is recorded by both the AC/S system and by the authentication equipment.

- Event time -

This is the time that the recorded event occurred. Sensor activations record an event when the activation begins and when the sensor activation ends. Other events, such as Start Acquisition, have only a single recorded event.

- Status -

An ON appearing in the status column marks the beginning of a sensor activation and an OFF status marks the end of sensor activation.

- Test -

When an event is the result of a test initiated by the authentication equipment, the word TEST displays in this column.

- EOM -

EOM means End of Memory and will mark the last record that was stored before the nonvolatile memory (NOVRAM) was filled. When the word YES appears in the EOM column there is sufficient memory space to record the end of Acquisition event, but any events that occur between the event marked with EOM and End of Acquisition are not recorded.

- Time>2 -

The time recorded with each event is the time read from the AC/S system, but that time is compared to the on-board clock in the authentication system. If the time difference between two systems is grater than two minutes for an event, YES displays in the Time>2 column.

- MD Test -

When a metal detector test is initiated, it displays in the Test column as described above. The reason for the test displays in the MD Test column. Metal detector tests are initiated on the basis of time intervals or a percentage of occupancies. The word TIME in the MD Test column indicated that the test resulted from a time interval and PERCENT indicates the test was based on a percentage of metal detector occupancies.

Clock Data

At the beginning of an acquisition period the authentication equipment clock is synchronized with the FCA system clock. The clock data before and after synchronization are stored in a clock file on the data diskette that is updated each time the diskette is used to start an acquisition period. The system user can view the clock data or print a hard copy to check the time difference between the two clocks before synchronization and to verify synchronization at the start of an acquisition period.

Self Test Data

Whenever a self test is performed on the authentication equipment, the test results are stored in a self test file on the data diskette. This diskette file is updated each time the self test is performed. The results of each self test displays with the time and date of the test.

Quit to Main Menu

Choose this option to return to the On-Site Services Main Menu.

3.7 Sort List Options

Sort List

When Acquisition Data has been selected from the Reports Menu and a data file has been chosen, a Sort List displays. The options allow the user to sort the data file three different ways. Once a selection is made from this list, the data displays in a scrollable region that can be reviewed on the computer monitor or printed.

Single Sensor

If user only interested in the history of a single sensor, this option chronologically sorts all events associated with the selected sensor. When this option is selected, a prompt asks the user to identify the sensor of interest from a list of available sensors in the data file that has been selected. After the user makes a choice, the data obtained from the chosen sensor displays.

Sensor ID

This option sorts the data chronologically, but groups the events according to the sensor identifications. For example, the events obtained from sensor A are listed chronologically followed by the events obtained from sensor B.

Chronological

The data is sorted and presented in the same order as it was collected. All events recorded during an acquisition period are included.

4. Other Considerations

4.1 Safety

The Authentication Controllers are powered from facility power. When the enclosure cover is removed, dangerous voltages are not exposed, except on the open frame power supply. Take care to avoid personal injury or damage to the equipment. The power supply is current limited and the battery output is fused at 3 amperes.

4.2 Error Messages

The following error messages are listed and a brief explanation given for each to aid the user in identifying the reason for an error message. Although many of these messages are extremely unlikely to occur, all of the known error message are listed in this list. The possible error messages are listed alphabetically and grouped according to the source of the messages. The DataKey messages are separated from the On-Site Services messages because they are generated by the DataKey interface module.

If you encounter an error message you cannot resolve, call Sandia National Laboratories for help.

4.2.1 On-Site Services Error Messages

An unexpected Datakey status was encountered.....

A Datakey response was received from the Authentication Controller when one was not expected. This is the problem internal to the controller.

Buffer could not be transmitted on COM 1.....

There is a serial communication problem. The problem is internal to the computer or the computer software.

Communications could not be established with CONTROLLER.

The computer software was unable to recognize that the communication cable was connected to an Authentication Controller. Repeat the attempt to establish communications, check the RS232 connections, and then run the Loopback test to identify the problem.

Communications verification has failed.....

The Authentication Controller responded to the computer, but the response did not contain the correct verification information. Check the serial communications cable and connections before making another attempt to establish communication.

Could not change to root directory.....

If the Report Generation routine could not change directories to go into the root directory, this message will appear. This indicates that there was a problem with the computer operating system.

Could not change to SCRATCH.FCA directory.....

The SCRATCH.FCA directory is a temporary directory created from the root directory of the computer. This message could only occur if the Report Generation software could not access this directory for some reason after it had been successfully created.

Could not CLOSE the data file.....

The computer cannot close the file on the diskette. The data may or may not be destroyed and the disk drive should be checked.

Could not create timer.....

This is a software timer used for many timing functions throughout the execution of the software. The software will not run unless the timer can be created.

Could not enable RTS/CTS Flow Control on COM 1.....

Serial communication handshaking is necessary to prevent the loss of data during data transfer. This message indicates a problem with the computer or its serial port.

Could not find README.FCA log file.....

This file is created or updated whenever data is downloaded to a data diskette. If it cannot be found on a diskette, the Report Generation software will not recognize it as a valid data diskette.

Could not find the loopback device after four attempts.....

If the loopback connector is actually in place, there is a problem with the serial port, the cable, or a connector.

Could not FLUSH the buffer to the data file.....

This message indicates that a problem was encountered during the execution of software in the computer.

Could not get the available space on the diskette.....

The software could not determine how much space is available on a diskette. Try another diskette.

Could not GET the current position in the data file.

This means that the data pointer information used to access data on the data diskette could not be retrieved. This may be a computer memory problem.

Could not make directory SCRATCH.FCA.....

The Report Generation routine was unable to create a temporary directory, SCRATCH.FCA, from the root directory of the computer.

Could not open the Communications port (COM 1).....

Serial communication port COM1 could not be opened. The serial port may be defective.

Could not OPEN the data tile.....

A file could not be opened on a data diskette. This could be caused by a defective diskette or disk drive.

Could not READ from the data file.....

Data could not be read from a diskette. The problem could be with the diskette or with the disk drive.

Could not SEEK to end of data file.....

The end of a data file could not be found. A corrupted diskette may be the cause.

Could not (SET / RESET) the Communications port (COM 1).....

The serial port COM1 cannot be set up with the correct communication protocol or cannot be returned to the original settings at the conclusion of the program.

Could not set the 3.5 inch drive to be the current drive.....

The software was not able to establish the 3.5 inch drive as the current drive. This is an internal computer problem and you will be locked out of any option that uses diskette operations.

Could not SET the current position in the data file.

This message means that the data pointer used to access the data on a data diskette could not be updated. This may be a computer memory problem.

Could not set the volume to (PORTAL / PENETRATION).....

The diskette could not be labeled as a P/M or PN/M data diskette. The most likely cause is a defective diskette.

Could not set to drive letter.....

The software was unable to set the working drive from the present drive to the drive indicated by the Drive Letter in the error message.

Could not WRITE to the data file.....

The software was unable to write to a file on the data diskette. A defective diskette is a probable cause of this error message.

Five (5) Datakey warnings have occurred.....

Five consecutive warning messages or unexpected returns have been read from the DataKey interface module.

Invalid Authentication Controller DATA diskette.....

This diskette is not recognized as a valid data diskette. An unformatted diskette or a data diskette with a corrupted disk structure causes this message to occur. The recommended action is to use a properly formatted data diskette in place of the diskette that caused this error message.

Invalid drive specified.....

The software was unable to communicate to the drive indicated by a keyboard response to determine how much available space was on the drive

Invalid Information was received from the Authentication Controller.....

The information received from the Authentication Controller contained data that was invalid. A check of the communication cable and connections should be made.

Invalid option specified for the Setup Port command.......

This message occurs if the software was unable to provide the correct parameters to the serial port controller.

MSDOS 3.3 or greater is not currently running on this system.....

If an old version of DOS is detected you will be returned to the DOS prompt.

The cable is not connected to Authentication Controller.....

Either the cable is not properly connected to the Authentication Controller or there is a problem with the cable connections. Connect the cable or check all the connections to COM 1.

The controller cannot communicate with the Datakey to program the parameters.

If this message appears there is a problem internal to the Authentication Controller. The controller is not communicating with its DataKey interface module.

The CONTROLLER was unable to recognize the command from the PC.....

The Authentication Controller received a message from the computer that it did not recognize. Since communication is obviously established, a momentary communication disruption is likely. Check the communication cable and retry the command.

The Date/Time information was Invalid.....

The date or time data received from the authentication controller contains out of range information such as day 0 or minute 65. Check the connections between the AC and the FCA clock outputs.

The Loopback device is not connected to the serial port.....

A loopback test was initiated, but the loopback connector was not detected at the COM1 port. Check the loopback connector and check all the connections to COM 1. If no problem can be discovered, the serial port may be defective.

The previous data has not been downloaded from the AC!!

The on-site services software has received a command to start acquisition, without having received a command to download data in the same session. The following message warns the user to be sure to save any data that must be retained: THE CURRENT DATA IN THE AC WILL BE LOST SHOULD YOU DECIDE TO CONTINUE!!!! If there is no need to save any previous acquisition data, the acquisition period can be started.

The printer is off line!
Put the printer on line and try the print again

A printer has been detected, but it is either turned off or is not on line.

There is no printer connected to the system!
The events cannot be printed

The software has tested for the presence of a printer and none has been detected. A printer must be attached to the computer parallel port before attempting to print a report.

The transmission from the CONTROLLER was not recognized.....

A message has been received from the authentication controller that was not a recognizable response. Since communication is obviously established, a momentary communication disruption is likely. Check the communication cable and retry the command.

There is not enough room on drive ....to hold all of the data.....

The drive indicated by a keyboard response did not have enough space available for the required function. Choose another drive.

Not enough room on the diskette to hold all of the data.....

The acquisition record to be downloaded to a data diskette is larger than the available space on the data diskette. Use an empty, formatted data diskette to complete the data download.

Diskette is unformatted or has a corrupted disk structure....

An unformatted or faulty diskette has been detected in the disk drive. Either format the diskette or replace it with another formatted diskette.

This is not a (PORTAL / PENETRATION) data diskette.......

The formatted data diskette in the disk drive was not formatted for the Authentication Controller with which it is being used. Reformat the diskette or substitute a correct data diskette.

This is not a valid Authentication Controller DATA diskette !

A formatted diskette has been detected in the disk drive, however it has not been formatted as a data diskette by using Diskette Services.

Timer timed out. Never received a response from the CONTROLLER.....

A message was sent to the Authentication Controller by the computer, but the response was not received and the On-Site Services software timed out. Check the communication cable between the computer and the AC.

Unexpected Error Number received.......

An error message that has not been anticipated has been received by the On-Site Services software from the computer operating system. Record the error number as it is displayed because this may be helpful in determining the cause.

With current information, there are no 3.5 inch drives connected to this system

The disk checking routines and the keyboard responses from the operator indicate that no 3.5 inch disk drives are resident in the computer. You will be locked out of any option that uses diskette operations.

4.2.2 DataKey Errors

COULD NOT DETERMINE THE DATAKEY RESPONSE CODE.

A response code identifies the type of data being sent by the DataKey interface module. This message probably indicates a problem internal to the Authentication Controller.

DATAKEY CONTACT INCOMPLETE

The DataKey is not making complete contact in the key receptacle. Check the DataKey for dirt or damage and re-insert.

DATAKEY DATA FILE IS NOT OPEN

An attempt has been made to access a data file that has not been opened. It is not likely that this message will occur while accessing the DataKey through the On-Site Services software.

DATAKEY INFORMATION ORGANIZATION ERROR

The data stored on the DataKey is not correctly organized. It is possible that removing the DataKey during the time that data was being written to it could cause this message.

DATAKEY SERIAL I/O TRANSMISSION ERROR

A framing or parity error occurred during the data transmission to the DataKey interface module. Electromagnetic interference or a faulty connection within the Authentication Controller are potential causes of this message.

INCOMPLETE DATAKEY COMMAND MESSAGE.....

The command message received by the DataKey interface module is invalid. This indicates a problem internal to the Authentication Controller.

INVALID DATAKEY DEVICE ADDRESS

The DataKey interface module has two ports and each has a unique address. This message indicates that the address was invalid. If this message occurs, there is serious communication trouble within the Authentication Controller.

NO DATAKEY PRESENT.....

There is no DataKey detected in the receptacle in the Authentication Controller. If a DataKey is in place, remove it and inspect the key for dirt or damage and try again.

THE DATAKEY DATA IDENTIFIER OR FILENAME SPECIFIED COULD NOT BE FOUND

An attempt has been made to open a DataKey file that does not exist on the key. The most likely reason for this error message is that the DataKey was not programmed for the particular Authentication Controller with which it is being used.

THE DATAKEY DATA IDENTIFIER SPECIFIED HAS ALREADY BEEN USED

An attempt has been made to open a file with a name that is already in use on the key. The DataKey was not properly Initialized during the programming process. Try again, but the DataKey interface module may be defective.

THE DATAKEY IS FULL

This message should not occur because the files used by the Authentication Controllers are very small and the keys are initialized with every use. If this message appears, there is a problem with either the DataKey or the interface module.

THE DATAKEY WAS REMOVED.

The DataKey has been removed during an operation. Make sure that the key is inserted properly and try again.

THERE WAS AN UNKNOWN DATAKEY ERROR:

A DataKey error code has been returned that does not match any expected error. In the unlikely event that this occurs, record the error number to help determine the cause.

4.3 Cautions

Exit All Other Software

The ONSITE software used with the authentication controllers can be operated on a variety of computers. The software has been tested on multiple computers with various configurations of hardware and software. However there are some situations which may cause problems. If a computer is normally operated with programs running in background, such as Sidekick or 1Dir, the reduction in available memory can cause symptoms ranging from DOS error message to a lockup of the computer. Before using ONSITE with a particular computer the user should check the AUTOEXEC.BAT and CONFIG.SYS files for assurance that no other problems are running simultaneously with ONSITE.

Toshiba Computers

There may also be compatibility problems between a computer and its operating system that can adversely affect the operation of ONSITE. An example of this was discovered while using a Toshiba 1200 laptop computer with Microsoft MSDOS 5.0. An apparent problem with ONSITE was traced to the fact that there are compatibility problems between Toshiba computers and MSDOS. For this reason, Toshiba markets its own operating system, Toshiba DOS, for use with Toshiba computers. Although this particular problem was eliminated, *it is recommended that only Toshiba DOS be used with Toshiba computers.*

Monitor Adjustment

ONSITE software can be run on either color monitors or monochrome monitors. If display contrast is poor and difficult to read on a monochrome monitor, particularly on some LCD displays, it may be helpful to change the DOS Mode parameters of the computer. Exit ONSITE and return to DOS. Then enter the following command from the DOS prompt:

```
C:>mode bw80
```

When ONSITE is restarted, the contrast should be improved and viewing the menus will be much easier.(You may also try the “onsite bw” command.)

Communication Errors

Errors that occur during communication with the Authentication Controller (cable disconnect, diskette problem) result in an error message display on the computer monitor. Such errors can be corrected with no interruption of the procedure if they are corrected within two minutes. If more than two minutes are required to correct the problem, the On-Site Services software returns to the menu from which the last option was selected.

Loss of Communication

In the event of a loss of communication (longer than two minutes) during a data download from the authentication equipment to the PC, the data diskette will contain only a portion of the acquisition data. The loss of communication that would most likely occur would be a disconnection of the cable between the PC and the controller. If this takes place during the data download process, the controller returns to its previous state and waits for a command from the PC. When the problem is corrected and the download procedure restarted, the On-Site Services software checks to see if there is sufficient space on the data diskette to hold the acquisition records. If not, the software prompts the user to insert a new data diskette. As a result, in order to protect the data and prevent losing a file that may be needed, there is a potential to cause some confusion to a user who examines the files recorded on the data diskettes. The user can see what files are stored on a data diskette with the List Files option of Diskette Services. If the file generated during an Interrupted download and a completed download file were stored on the same data diskette, it appears that two files existed for the same acquisition period, except that the complete file is longer. A similar situation occurs if the two files were stored on different disks. If an incomplete download is followed by a complete download, the Comment Field in the scrollable region indicates the total number of data blocks in the record file and the number of blocks that were actually downloaded.

Power Loss

If power to the P/M or PN/M Junction Unit is turned off for periods of time greater than three hours, disconnect the authentication equipment battery by removing the fuse F1 on power supply board to avoid completely discharging the battery. The battery used in the Authentication Controllers should not be damaged by deep discharging, even for periods of up to one month. To assure battery reliability, follow the procedure above.

4.4 Troubleshooting

Troubleshooting suggestions will be made according to the symptoms that may be observed. The equipment is modular and component level Troubleshooting suggestions will not be attempted.

Communication Problems

Communication cannot be established with authentication equipment

The source of the problem should be identified and this can be accomplished rather quickly by means of the Loop-Back Test option on the Main Menu. This option should be used in conjunction with a loop-back connector attached to the computer COM1 port or at the end of the communication cable connected to the COM1 port. If the loop-back connectors provided with the equipment are not available, replacements can be made by connecting the TD pin to the RD pin, the RTS pin to the CTS pin, and the DTR pin to the DSR pin on a connector that mates to the computer COM 1 port or to the communication cable connector. Wiring diagrams for the serial communication cable and the loop-back connectors are in the Maintenance section of this manual. When a loop-back connector is attached to COM 1 the computer I/O functions can be checked by means of the Loop-Back Test option. A failure of this test indicates that the problem is within the computer. If no problem is indicated, the communication cable can be checked by plugging one end into the COM1 port and the other end into a loop-back connector. Running the Loop-Back Test with this equipment configuration will test both the computer and the communication cable.

If the computer and the communication cable pass the Loop-Back Test, then the Authentication Controller is suspect. A simple test at this point would be to attempt to establish communications with both Authentication Controllers using the same computer and communications cable. If communication can be established with one controller and not the other, then the problem is in the Authentication Controller.

Fix Authentication Controller

Authentication Controller does not function

Remove the enclosure cover and check voltages on the power buses near the power supply board. If the 5V bus measures less than 5 VDC, then check to see If AC power is available to the power supply. If AC power is not present or if the DC power supply fails, the battery will only provide power for approximately three hours. If there is a short circuit on the power supply output it will shut down and appear to be malfunctioning. There is a fuse in the power supply module and also a 3A fuse, F1, on the power supply board.

Before attempting to remove the Authentication Controller chassis from the enclosure or before troubleshooting the controller, remove power from the unit by disengaging the AC power connector J4 and by removing the DC fuse F1 on the power supply board.

Sensor Test Problems

Sensor or sensors repeatedly fail self test

If the sensor appears to be functioning correctly, but still fails the self test, check the wiring from the Junction Unit to the Authentication Controller. Next, check the wiring between the controller connector and the I/O board. If the wiring appears to be in order, monitor the relay output during a self test to check the operation of the relay on the I/O board.

Memory Self Test

Authentication memory fails self test

The memory check tests both the on-board RAM and the non-volatile memory cartridge (NOVRAM). Replace the NOVRAM cartridge by pulling out the suspect cartridge and plugging in a replacement. The RAM chip on board the microprocessor board is socketed and is relatively easy to replace also. Since these parts are either socketed or plugged into a connector, before replacing either one it would be worthwhile to reinsert the components after checking the contacts. The NOVRAM connector wiring should be inspected if replacement of the cartridge does not correct a NOVRAM failure.

4.5 Maintenance

The Authentication Controllers are designed to operate unattended and to require a minimum of maintenance. Replaceable components are the battery output fuse, F1, the system battery, and the non-volatile RAM (NOVRAM) cartridge. The memory cartridge and the battery each have a minimum life of five years. The NOVRAM cartridge is accessible when the enclosure cover is open and can be removed and replaced any time the system is not in acquisition. Replacement of the battery requires some disassembly and the chassis must be removed from the enclosure. Disable all power sources before removing the chassis from the enclosure. Disconnect the power connector J4 to isolate AC power, and remove F1 from the power supply board to isolate the battery.

Wiring Diagrams

Serial Communication Cable

IBM AT COM 1 (DE-9S)			Authentication Controller RS232 connector (DB-25P)	
RxD	3	———	2	RxD
TxD	2	———	3	TxD
RTS	7	———	4	RTS
CTS	8	———	5	CTS
DSR	6	———	6	DSR
Gnd	5	———	7	Gnd
DTR	4	———	20	DTR

Loop-Back Connector COM 1 (DE-9S)		Loop-Back Connector COM 1 (DB-25S)	
TxD	2 ┐	┌2	TxD
RxD	3 ┘	└3	RxD
DTR	4 ┐	┌4	RTS
DSR	6 ┘	└5	CTS
RTS	7 ┐	┌6	DSR
CTS	8 ┘	└20	DTR

Note: These diagrams are applicable to IBM AT and Toshiba T1600 computers and cannot be applied universally. The information provided here is for reference and as a guide for adaptation to other machines.

This is a blank page.

FCA AUTHENTICATION SYSTEM

AUTOMATIC COMPARATOR MANUAL

Sandia National Laboratories
Novenber,1992

Table of Contents

FCA Authentication System

Automatic Comparator Manual

1. Introduction

The Automatic Comparator is a software package that is designed for use with the authentication equipment at the Fast Critical Assembly (FCA) facility operated by the Japan Atomic Energy Research Institute (JAERI). The Authentication Controllers at the FCA facility independently monitor sensor inputs from the Advanced Containment and Surveillance (AC/S) system and record sensor activity data until it is downloaded to an International Atomic Energy Agency (IAEA) computer operating with the ONSITE software. The data can be displayed on the computer screen or printed using only the ONSITE software. An inspector can manually compare that data to the data record produced by the JAERI AC/S system, but the large number of event records that must be checked make that process unwieldy. To aid the inspectors in this process the Automatic Comparator program was written to allow a computer comparison of the two data records.

2. Equipment

2.1 Software

The software is provided on one 3.5 inch disk to enable an IAEA inspector to do a data comparison with the same personal computer that is used to download the data from the Authentication Controllers. The comparator software can be operated on other computers as long as they conform to the hardware requirements described in Section 2.2.

2.2 Hardware

The specifications for a computer that can be used to make FCA data comparisons with the Automatic Comparator software are similar to the requirements for the computer that is used to run the ONSITE software.

Personal computer requirements:

- Fully IBM compatible

- MS – DOS 3.3 (or higher) operating system
- 640K RAM minimum
- Centronics compatible parallel port
- One 3.5 inch 720KB or 1.44 MB disk drive
- A hard disk or RAM drive with 2 MB free for use by comparator software

3. Techniques and Procedures

3.1 Installation and Setup

Procedure

1. Turn on the computer.
2. Go to a DOS prompt, for example C:, if one is not displaying already. (If you have Windows or a menu system that displays when you turn on the computer, you must exit to DOS.)
3. Insert the Automatic Comparator diskette into the appropriate drive. (Do NOT insert the disk into a drive before turning on the computer. The comparator diskette is not bootable.)
4. Type the drive name, a colon, and then press ENTER (for example, A:).
5. To start the software, type the command FCACOMP and press ENTER (for example, A: >fcacomp).

Monitor Settings

When the FCACOMP command is entered, the software defaults to either color or monochrome (black and white) depending upon the computer set-up. The user can choose to run the program in either color or monochrome by entering the command “fcacomp color” or “fcacomp bw”. When FCACOMP is run on a laptop computer with a LCD screen, use the “onsite bw” command to improve the contrast.

Using the Hard Disk

Use this procedure if the software has been installed on the hard disk:

1. Change directory to directory containing the software.
2. Type the command FCACOMP. A “Checking floppy drive...” message appears while the software checks for the existence of a 3.5 inch floppy disk drive. When there is a diskette in the drive (assuming that there is a

3.5 inch drive) the software immediately displays the title screen. If there is no diskette in the drive a DOS error message may appear on the screen indicating an error reading the drive. (This response depends on the model of computer and its hardware configuration.) The user has two options at this point:

- Insert a data diskette into the drive and type a Retry keyboard response (R) to advance the software to the title screen, or
- If the user does not wish to insert a data diskette into the disk drive at this time, a Retry (R) or Abort (A) response from the keyboard will also bring up the title screen. Due to differences among computers the keyboard response which causes the program to advance to the title screen may vary, but one or more of the three responses (Abort, Retry, or Fail) will successfully clear this DOS message.

Set Date and Time

When the program runs, a title screen appears and the user can verify or correct the date and time information. Pressing the up and down arrow keys on the computer keyboard lets the user select either the date or time. The user may enter the correct values, if necessary. Press the ENTER key to record the changes or confirm that the existing values are acceptable. The current system date and time appear at the top of the screen.

Disk Space Check

After the time and date are set, the program checks drive C to determine if at least 2 megabytes of disk space is available for temporary files. If there is sufficient space on drive C, the program execution proceeds without interruption. If there is insufficient space on drive C, the user is asked to identify a disk driver or RAM drive that the comparator software can use.

3.2 Operating Instructions

Key Information

Instructions for the user and descriptions of key functions display at the bottom of the screen. Press F1 to call the HELP utility to provide additional instruction about the current screen.

Press the ESC key to end the program or stop a print operation in progress.

Insert Authentication Data Diskette

After the program sets up a "scratch drive" for temporary files, it prompts the user to insert an authentication data diskette. If the diskette inserted into the designated drive is not an authentication data diskette, a warning banner alerts the user and gives instructions about how to proceed. The diskette may be replaced with an appropriate data diskette to proceed or the program may be terminated.

File Display

The comparator software reads the authentication data diskette and displays the files that are present on the diskette. To select a file, use the arrow keys to highlight the desired file and press ENTER. After the comparator program copies the chosen file to the scratch area, the system prompts the user to remove the authentication diskette from the disk drive.

Insert AC/S data diskette

Upon removal of the authentication data diskette, the program asks the user to insert an AC/S data diskette into the disk drive. This data diskette should contain data from the same inspection period as the file selected from the authentication data diskette. If the wrong type of data diskette (or no diskette) is present in the disk drive when any key is pressed on the keyboard, the user is prompted to either correct the situation or to exit the program.

Program Results

After the AC/S data files are copied from the diskette, a prompt tells the user to remove the diskette. The software compares the data form the two diskettes and displays the results of comparison. Use the arrow keys to scroll through the displayed records. The records can be printed if a printer is connected to the parallel printer port of the computer. In the event that more than 800 unmatched events result from the data comparison, the entire listing may not display on the computer screen, but the records can still be printed in their entirety. If there are no unmatched events found during a data comparison, a screen message displays that information and any Alert messages (see Section 3.3) that result from the data comparison.

Exit

After the unmatched events display, the program execution is complete. Exit the program by pressing the ESC key. Restart the program if further data comparisons need to be made.

3.3 Alert Messages

When the comparison of the two data diskettes is complete, the unmatched events display in a scrollable region on the computer screen. There are three conditions that may cause a highlighted alert message to appear above or below the scrollable region:

There were records that have a time difference of greater than 2 minutes!

The automatic comparator software encountered one or more events in the authentication record that had a 'Time>2' flag. That flag is attached to an event when the Authentication Controller clock and the AC/S system clock are more than two minutes out of synchronization. A review of the authentication data and the clock synchronization data will reveal the number of records involved and the clock data at the beginning of the inspection period. See section 3.6 of the *FCA Authentication System Operator's Manual* for more information.

An End of Memory condition occurred during this reporting period!

The non-volatile memory cartridge in the Authentication Controller filled up during the inspection period. No data was recorded after the event that contains this flag except for the End of Acquisition record. See section 3.6 of the *FCA Authentication System Operator's Manual* for more information.

There are more records in the file than can be displayed!

Approximately 800 unmatched events .can be displayed in the scrollable region on the computer screen. The message indicates that there are more events in the unmatched file than can displayed on the computer. To see the complete list of unmatched events, the user must print out the records.

4. Other Considerations

4.1 Error and Warning Messages

Two kinds of messages display to indicate that a problem has occurred:

- A **Warning** message appears when a recoverable problem has occurred and offers suggestions for resolving the problem.
- **Error messages** are fatal and give the user an explanation of the source of the problem before existing the software and returning to DOS.

The following list of Error and Warning messages is provided to aid the user in determining the reason for a particular message and to suggest possible actions that should be taken.

4.1.1. Error Messages

The following list of error messages provides a brief explanation to help the user identify the reason for an error message. Although many of these messages are extremely unlikely to occur, all known error messages are included in the list. The error messages are listed alphabetically.

Could not change to root directory...

The program cannot change directories to go into the root directory. There is a problem with the computer operating system.

Could not change to SCRATCH.FCA directory...

The SCRATCH.FCA directory is a temporary directory created from the root directory of the computer. This message occurs if the comparator software connot access this directory for some reason after it has been successfully created.

Could not CLOSE data file <FILENAME>

The computer cannot close a file on the diskette. The data may or may not be destroyed and the disk drive should be checked.

Could not CREATE file <FILENAME> in the scratch area

The program cannot create a file in the SCRATCH.FCA directory.

Could not create the temporary file in the scratch area...

The program cannot create a file in the SCRATCH.FCA directory.

Could not DELETE file <FILENAME> from the scratch area...

The program is not able to delete a file that it has created in the SCRATCH.FCA directory.

Could not GET the current position in the data file...

The data pointer information used to access data on the data diskette could not be retrieved. This may be a computer memory problem.

Could not make directory SCRATCH.FCA...

The comparator program was unable to create a temporary directory, SCRATCH.FCA, from the root directory of the computer. The directory may already exist, or there may be an operating system problem.

Could not OPEN file <FILENAME>...

A file could not be opened on a data diskette. This could be caused by a defective diskette or disk drive.

Could not READ from file <FILENAME>...

Data could not be read from a diskette. The problem could be with the diskette or with the disk drive.

Could not remove directory SCRATCH.FCA...
The SCRATCH.FCA directory may still exist when you exit the program...

Since this message occurs after the data comparison is completed, the only immediate concern is to delete the SCRATCH.FCA directory from the computer. However , there may be a problem with the computer or disk drive.

Could not RENAME the temporary file...

The temporary files in the scratch directory cannot be renamed by the comparator program. The most likely cause is that an old version of the SCRATCH.FCA directory exists. Exit the FCACOMP program to remove SCRATCH.FCA, and restart the comparison program. A less likely cause of this message is a defect of the computer or disk drive.

Could not SEEK to end of data file...

The end of data file could not be found. A corrupted diskette may be the cause.

Could not set the 3.5 inch drive to be the current drive...

The software was not able to establish the 3.5 drive as the current drive. This is an internal computer problem and the program execution cannot continue.

Could not SET the current position in the data file...

The data pointer used to access the data on a data diskette could not be updated. This may be a computer memory problem.

Could not set the drive to <DRIVELETTER>

The software was unable to set the working drive from the present drive to the drive indicated by the Drive Letter in the error message.

Could not set the TIME ZONE environment variable.

This message refers to the initialization of a program variable in the comparator software. It is a fatal error because this variable is used to convert the AC/S time and date to the same format as the authentication data.

Could not set to scratch drive <DRIVELETTER>

The software was unable to set the working drive from the present drive to the scratch drive indicated by the Drive Letter in the error message.

Could not WRITE to file <FILENAME> in the scratch area...

The software was unable to write to a file in SCRATCH.FCA directory. Defective media in the scratch drive is a probable cause of the problem.

Drive <DRIVELETTER> is invalid...
Could not get the available space.

The software was unable to communicate with the drive you selected to determine how much available space was on the drive.

FUNCTION: <FUNCTIONNAME> illegal function call!

Since function calls are made by the software, this message indicates serious problems with the program execution. Corruption of the software or a memory defect are possible causes.

MS-DOS 3.3 or greater is not currently running on this system...

If an old version of DOS is detected you will be returned to the DOS prompt.

The printer is OFF LINE!
Put the printer ON LINE and try again...

A printer has been detected, but it is either turned off or is not on line.

There are NO data files on the diskette!

The data diskette does not have the expected data files to use for data comparison.

There is insufficient system memory to display the data file choices form...

There is not enough computer memory available to display this information. Check to see if the computer meets the specifications in section 2.2. This may be a computer memory problem.

There is no printer connected to this system!
The unmatched events cannot be printed.

The software has tested for the presence of a printer and none has been detected. A printer must be attached to the computer's parallel port before attempting to print a report.

There is not enough memory in this system to complete the task...

There is not enough computer memory available to carry out this task. Check to see if the computer meets the specifications in section 2.2. This may be a computer memory problem.

Unexpected EOF reached while reading the <FILENAME> file...

An end of file marker has been encountered in an unexpected location. The file may be corrupted.

With current information, there are no 3.5 in. drives connected to this system.

The disk checking routines and the keyboard responses from the operator indicate that no 3.5 inch disk drives are resident in the computer.

4.1.2 Warning Messages

Warning messages do not necessarily end the program execution. Corrective action can solve the problem in many instances. The warning messages often offer suggestions on how to solve the problem.

Could not find README.FCA log file...
This diskette is considered corrupt.
If continuing, please try another Authentication Data diskette.

The README.FCA file is created or updated whenever data is downloaded to a data diskette. If it cannot be found on a diskette, the diskette is not recognized as a valid data diskette.

Drive does not contain a floppy!
If continuing, please insert a valid data diskette in the drive...

The program cannot detect a diskette in the specified disk drive. If a diskette is in the drive, remove it and re-insert the diskette. If this does not correct the problem the drive may be defective.

Drive does not contain media...
Please insert the proper media into the drive...

The program cannot detect the expected media in the specified drive. If the media (Bernoulli cartridge, for example) is in the drive, remove and re-insert it. If this does not correct the problem the drive may be defective.

Invalid Authentication Controller data diskette...
Please insert a valid Authentication Controller data diskette into drive...

This diskette is not recognized as a valid data diskette. Check to make sure that the diskette is labeled as an authentication data diskette. An unformatted diskette or a data diskette with a corrupted disk structure also causes this message.

The data on the diskette in drive <DRIVELETTER> does not fall within the date of the inspection period being compared!
If continuing, please try the proper AC/s data diskette.

The data on the AC/S data diskette is outside the beginning and ending dates of the data on the authentication data diskette used for comparison. Check the inspection period dates on both diskettes to make sure they correspond.

The diskette in drive <DRIVELETTER> is not an AC/S <PORTAL or PENETRATION> data diskette!
Please insert the proper corresponding AC/S data diskette in the drive...

The comparator software has detected either a Portal or Penetration data diskette when it was expecting the other (Penetration or Portal). Check to make sure that the correct data diskette is being used.

The diskette in drive <DRIVELETTER> is unformatted or has an unknown format!
Please insert a valid data diskette in the drive...

An unformatted or faulty diskette has been detected in the disk drive.

The media in drive <DRIVELETTER> is WRITE PROTECTED...
Please remove the write protection to proceed...

The drive you told the software to use for a scratch area is write protected. Remove the write protection so that a scratch directory can be created.

The start or end time of the data does not fall within + or – TIMEWINDOW minutes of the inspection period being compared!
If trying another diskette, replace the diskette before hitting 'T'.

The difference in time between the start or end times of the authentication data and the AC/S data exceeds the time window that appears in the warning message. The comparison can still be carried out, but some events may be unmatched or left out of the comparison process depending on which system starts or ends first.

There is not enough room on drive to hold all of the data...

The drive indicated by a keyboard response does not have enough space available for the required function.

4.2 Troubleshooting

Problems that occur while the software is running generate Error and Warning messages that indicate the source of the problem and possible solutions.
Computer and drive problems may be isolated by running the software on a different computer. Backup copies of the data diskettes can be made using the DOS DIKCOPY command, but data files cannot be copied individually from one diskette to another. The FCACOMP Program (FCACOMP.EXE) should be backed up to prepare for the possibility that the working copy might become corrupted.

FCA AUTHENTICATION SYSTEM

DATAKEY OPERATIONS MANUAL

Sandia National Laboratories
November, 1992

Table of Contents

FCA Authentication System

DataKey Operations Manual

1. Introduction

The Fast Critical Assembly (FCA) Authentication Controllers are programmed with operating parameters that are transferred from the International Atomic Energy Agency (IAEA) Regional Office to the FCA facility on a DataKey. The DataKey is an EEPROM device which is easily carried to the facility by an IAEA inspector. The operating parameters of both the Portal Monitor and the Penetration Monitor Authentication Controllers can be stored on a single DataKey by an inspector prior to leaving the IAEA Regional Office. The purpose of the DataKey is to provide a secure and rugged means of transporting the operating parameters of the authentication equipment to the FCA facility. When the DataKey is used together with software resident in the IAEA inspector's personal computer, the authentication controllers can be reprogrammed. However, neither the DataKey nor the computer alone can be used to change the operating parameters of the controllers.

This manual describes the operation of the DataKey programming software and procedures that normally take place at the IAEA Regional Office rather than on-site at the FCA facility.

2. Equipment

2.1 Software

The software is provided on one 3.5 inch disk to permit a personal computer to operate with a Datakey interface module to program the DataKeys. Because the software permits any user to program DataKeys, it is important to protect the software and control its use.

2.2 Hardware

The hardware requirements are:

Personal computer

- Fully IBM compatible
- MSDOS 3.3 or higher operating system
- 640K RAM minimum
- One RS232 serial communication port (COM 1)
- One 3.5 inch 720 KB or 1.44 MB disk drive

Datakey Interface Module SKS-232A

RS232 cable to connect computer to SKS-232A

- Computer end must mate to COM 1 serial port
- Interface module end must be a DB-25P connector or equivalent

Serial Data Keys

- Datakey models DK1000, DK2000 or DK4000 may be used

3. Techniques and Procedures

3.1 Installation and Setup

Procedure

1. Connect the serial communications port COM1 to the DataKey Interface Module with an RS232 cable.
2. Turn on the computer.
3. Go to a DOS prompt, for example C:/>,if one is not displaying already. (If you have Windows or a menu system that displays when you turn on the computer, you must exit to DOS.)
4. Insert the disk into the appropriate drive. (Do NOT insert the disk into a drive before turning on the computer. The DataKey software disk is not bootable.)
5. Type the drive name, a colon, and then press ENTER (for example, A:).
6. To start the software, type the command PROGDKEY and press ENTER (for example, A:>progdkey). When the program runs, a title screen displays.
7. Verify or correct the date and time information. Press the up or down arrow keys to select either the date or time. You may enter the correct values, if necessary. Press the ENTER key to record the changes or confirm that the

existing values are acceptable.

After the user has typed new values or accepted the current values of date and time, the Main Menu displays. The current system date and time appear at the top of the screen.

Using DataKeys

To store information on the DataKey, insert the key into the DataKey receptacle on the front of the Datakey Interface Module. Next, rotate the key 90° in a clockwise direction or until it stops. The system software checks for proper communication with the DataKey and prompts the user to take corrective action if there is a communication failure. After programming a DataKey with the desired information, remove it from the interface module by rotating the key counterclockwise and pulling the key out of the module socket.

3.2 Operating Instructions

Help

A HELP utility is always available. Press F1 to call the HELP utility, which provides additional instruction about the current menu selection.

Main Menu

The Main Menu initially lets the user select one of three options:

1. The **Portal Monitor** option guides the user through the choices required to store operating parameters necessary to program the Portal Monitor Authentication Controller.
2. The **Penetration Monitor** option lets the user select Penetration Monitor Authentication Controller parameters, and store those selections on a DataKey.
3. **To exit** the DataKey programming software, the user selects the third option to return control to the computer operating system.

Parameters

Normally, one DataKey can store the operating parameters for both Authentication Controllers at the FCA facility. Therefore, when the operating parameters for one of the controllers (Portal or Penetration Monitor) have been stored on a key, that Main Menu selection is locked out and only the remaining option(s) can be selected. If a change must be made to the data that has been stored on a DataKey, simply re-enter the program and store the desired parameters on the same DataKey. The software automatically initializes the key and erases all previously stored data.

Key Functions

Instructions for the user and descriptions of the operations of F1, F2, F3, and ECSCAPE keys display at the bottom of the screen. Press the F6 key to erase the field indicated by the cursor position on any of the software menus. Press the F7 and F8 keys to move the cursor back one field or forward one field respectively. The F7 and F8 keys are similar (but not identical) in function to the left and right arrow keys.

3.3 Portal Monitor Option

Menu Choices

Select the Portal Monitor option to display the Portal Monitor Choices menu. The Authentication Controller can monitor 0 to 3 sensors in the Portal Monitor in addition to randomly testing the metal detector MD1. The choices are:

- the selection of the number of sensors to passively monitor,
- which sensors will be monitored, and
- how the random metal detector testing will be accomplished.

Choosing and Identifying Sensors

The first choice is the number of sensors to monitor in addition to the metal detector which is always monitored. Press F2 to display a list of possible choices. If the user already knows the appropriate response, the user can type the selection immediately. If the user types an inappropriate response, the choice list automatically displays and the user can make a selection from that list. After the user selects the number of sensors, the user can identify the sensors to be monitored. The software does not permit the number of sensor designations to differ from the number of sensors selected to be monitored.

Metal Detector Test

The metal detector test occurs randomly based on a percentage of occupancies, during a specified period of time, both, or neither. The user may select a percentage and a time interval. To eliminate a test mode, type zero.

Changing Information

After all choices have been made, the user can use the arrow keys to move the cursor and change any of the selections. If the number of sensors is changed, the sensor designations must be re-entered.

Storing Choices

When all changes have been made and the you are satisfied that the operating parameters of the Portal Monitor Authentication Controller are correct, press the F3 key to store the choices on the DataKey. The software initializes the computer communications port and check for proper operation of the Interface Module. The user may be asked to check the RS232 cable, plug in the Interface module, or to insert a DataKey into the module. These instructions appears as Warning Messages at the bottom of the computer screen. The system displays a verification message when the operating parameters have been successfully written to the DataKey. the user is instructed to return to the Main Menu. When the Main Menu displays, the Portal Monitor option is no longer available because this information has already been written to the DataKey.

3.4 Penetration Monitor Option

Menu Choices

Select the Penetration Monitor option from the Main Menu to view the Penetration Monitor Choices menu. First, the user must select the number of sensors to be monitored by the Authentication Controller. Up to three sensors can be passively monitored, and a subset of those sensors can also.be selected for random testing. For example, if three sensors are chosen to be monitored, then any or all of those three can also be chosen to be randomly tested, but no other sensors can be randomly tested.

Random Tests

The random tests conducted at the Penetration Monitor are not actual tests of the sensors, but rather of the data gathering equipment. While the metal detector tests initiated by the Portal Monitor Authentication Controller are active tests of the metal detector, the tests initiated by the Penetration Monitor Authentication Controller are *simulated sensor activations.*

Choosing Sensors

When the number of sensors to be monitored is selected, a corresponding number of sensor identifications must be made. Type the sensor IDs, if known, or press F2 to display a Choice List of valid sensor IDs. If you type an invalid ID, or if you press ENTER without typing a sensor ID, the Choice List displays automatically. Make a selection from the list by moving the cursor to the desired selection and pressing the ENTER key.

Actively Tested Sensors

The user does not have to enter any sensor IDs in the Actively Tested Sensors block, but pressing F2 activates a list of sensors that can be chosen to be randomly tested. Only the sensors selected for passive monitoring are valid choices. Type the sensor IDs or select them from the choice list by moving the cursor with the arrow keys to the correct sensor and pressing the ENTER key. If you press the ENTER key without making a selection, no sensors will be tested.

Time Interval

The last choice on this screen is the Time Interval. This determines the frequency of the random tests. If no sensors have been chosen, this field is locked out and no selection can be made.

Changing and Storing Choices

Changes can be made to the entries on this screen by using the arrow keys to move the cursor to select the field to be edited. After the user is satisfied that the correct parameters are displayed on the screen, press the F3 key to program the DataKey with the information as described in the Portal Monitor Option section.

Main Menu options

When the user returns to the Main Menu, only options not previously used are available. If both the Portal Monitor and the Penetration Monitor options have been used, the only available option is to Quit to DOS.

3.5 Quit to DOS Option

Any time the user returns to the Main Menu, the user may leave the DataKey software and return to the computer operating system. However, the DataKey cannot be partially programmed with the intention of completing the procedure during another session. When starting up the software program to load any operating parameters on the DataKey, all previously stored information is erased.

NOTE: All data to be stored on a DataKey must be recorded in a single session.

4. Other Considerations

4.1 Error Messages, Warnings

Two kinds of messages display to indicate that a problem has occurred during execution of the software. A Warning Message appears when a recoverable problem occurs and offers suggestions for resolving the problem. Error messages, however, are fatal and give the user an explanation for the source of the problem before exiting the software and returning to DOS. The following list of Error and Warning Messages is divided into sections depending on the source and severity of the problem.

If you need help for fatal problems, call Sandia National Laboratories.

DataKey Warning Messages (recoverable)

DATAKEY CONTACT INCOMPLETE

The DataKey contacts may be dirty or damaged. Remove the DataKey, check for dirt or damage and reinsert.

INVALID DATAKEY DEVICE ADDRESS

The Interface Module device address is incorrect (not Hex 00 for port 0 or Hex 01 for port 1).

NO DATAKEY PRESENT

The system cannot detect the presence of a DataKey in the Interface Module.

SERIAL I/O TRANSMISSION ERROR

There has been an error detected in the serial communication.

THE DATAKEY WAS REMOVED

This message could appear if the DataKey was removed during an operation.

DataKey Error Messages (fatal)

COULD NOT DETERMINE RESPONSE CODE

A response code is a message from the DataKey Interface Module. An unexpected response was received.

DATA FILE IS NOT OPEN

There was an attempt to access a file that has not been opened first.

INCOMPLETE COMMAND MESSAGE

The command message from the computer was invalid or incomplete.

KEY INFORMATION ORGANIZATION ERROR

The file data on the DataKey does not checksum properly. It is possible that removing the DataKey during the time that data was being written to it could cause this message.

THE DATA IDENTIFIER OR FILENAME SPECIFIED COULD NOT BE FOUND

An attempt has been made to open a DataKey file that does not exist on the key.

THE DATA IDENTIFIER SPECIFIED HAS ALREADY BEEN USED

An attempt has been made to create a file that is already in use. The DataKey was not properly initialized during the programming process. Try again, but the DataKey interface module may be defective.

THE DATA KEY IS FULL

This message is unlikely to occur because the files are very small and the keys are initialized at every use. There is a problem with the DataKey or the interface module.

THERE WAS AN UNKNOWN ERROR: < Error Number >

This message was created in the event that a problem occurs that was not foreseen.

System Error Messages (fatal)

COULD NOT CONVERT USER CHOICES

The software could not convert the user choices to DataKey commands.

COULD NOT CREATE RECEIVE TIMER

The timer which is used to timeout system responses is not functioning properly.

VERIFY FAILED

The data written to a DataKey would not verify correctly and so is not reliable.

Communication Warning Messages (recoverable)

THE CABLE IS NOT CONNECTED TO COM1 OR THERE IS NO POWER TO THE DATAKEY

The computer is unable to get a response from the Interface Module. The user has five tries to re-establish communications.

TIMER TIMED OUT. NEVER RECEIVED THE RESPONSE FROM THE DATAKEY

During communication with the Interface Module a response must be received within 10 seconds. If the timer times out, this message appears.

PROGRAM EXECUTION WILL CONTINUE.. DATA WILL BE VERIFIED SHORTLY.

If the previous message (TIMER TIMED OUT...) appears during the write operation, this message appears before the data is verified.

Communication Error Messages (fatal)

BUFFER COULD NOT BE TRANSMITTED ON COM1

This means that the data to be transmitted could not be sent to the COM1 port of the computer.

COMMUNICATIONS WITH THE DATAKEY COULD NOT BE ESTABLISHED (COM1)

After five attempts by the user to establish communications with the Interface Module, this message appears before the software returns control to DOS.

COULD NOT CONFIGURE THE COMMUNICATIONS PORT (COM1)

This indicates that a problem was encountered while setting up communications protocol on COM1.

COULD NOT ENABLE RTS/CTS FLOW CONTROL ON COM1

The serial port handshaking procedures are not operating correctly.

COULD NOT OPEN THE COMMUNICATIONS PORT (COM1)

The COM1 serial port is not available for use by the system.

THE PREVIOUS WARNING HAS OCCURRED FIVE (5) CONSECUTIVE TIMES

When five unsuccessful attempts have been made to resolve a problem, this message appears before the user returns automatically to DOS.

TIMER TIMED OUT. NEVER RECEIVED THE RESPONSE FROM THE DATAKEY

This is a fatal error if the problem occurs when the software unsuccessfully attempts to open a file on the DataKey.

4.2 Troubleshooting

Problems that occur while the software is running generate Error and Warning Messages that indicate the source of the problem and possible solutions. The user has five attempts to rectify the problem before the program automatically returns to DOS. Areas of potential problems are:

RS232 cable

An RS232 serial communications cable must connect the computer COM1 port to the Datakey Interface Module connector. Some serial communications cables exchange pins 2 and 3 from one end to the other, and if such a cable is used, proper communication cannot be established. Pin 2 at one end of the cable should be connected to pin 2 at the other end, and pin 3 must be connected to pin 3 in the same manner.

COM1 port

Depending on what kind of computer is being used to program the DataKeys, the COM1 port connector may require different mating connectors. Typically the COM1 port will be either a 9-pin or a 25-pin connector, but it may require either socket or pin connections on the mating connector. Regardless of what kind of connection is required it is important to remember that the software will only communicate with the Datakey Interface Module over COM1, and no other port can be substituted. If another device is connected to COM1, for example, a mouse or a modem, it must be taken out of service before attempting to use the computer to program DataKeys for use with the FCA Authentication Controllers.

AC Power

The Datakey Interface Module will operate from 85 to 120 VAC at either 50 or 60 Hz with the wall mount power adapter provided. If this is properly plugged into mains power and into the power receptacle on the module box, the Interface Module should operate normally.

This is a blank page.

FCA AUTHENTICATION SYSTEM

TECHNICAL MANUAL

Sandia National Laboratories
November, 1992

Table of Contents

Figures

Tables

Drawings

FCA Authentication System
Technical Manual

1. Introduction

Overview

The Authentication Controllers are microprocessor controlled data collection systems with output capabilities that permit the initiation of random AC/S system tests and serial communication to authorized computer equipment. The system design is modular and consists largely of commercially available components. Manufacturer's data sheets for commercial products used in the authentication system design are not included in this manual (see another brochure).

An IBM compatible computer running ONSITE software is required to communicate with the authentication equipment and to collect the stored data. Operating parameters can be programmed into the authentication equipment by means of a DataKey, an EEPROM device that is used in conjunction with computer. A DataKey interface module and the PROGDKEY software needed to program the parameters onto a DataKey are provided with the system.

The inspector's PC must have 2 Mbytes of hard disk space available for On-Site Services software. During report generation procedures, the software creates a temporary directory in that disk space. However, the system erases and removes the directory at the conclusion of the work session.

The maintenance procedures that are described in this manual should not be attempted while the Authentication Controllers are in acquisition. Throughout these procedures, the front of the chassis refers to the side where the RS232 and DataKey connectors are located. Right and left directions assume that the chassis is viewed from the front(see Figure 1).

2. System Description

Although the PN/M Authentication Controller and the P/M Authentication Controller are very similar, there are some physical differences. The P/M Authentication Controller has one more isolated I/O board than the PN/M Authentication Controller, and there are two metal detector test buttons found only in the P/M Authentication Controller. The software that is resident in the two controllers is quit different, but since they are physically similar, descriptions of the Authentication

Controllers make no distinction between the two except for those already noted.

2.1 Power Supply

The AC Power supply is universal input commercial power supply manufactured by Converter Concepts. The model WI25-241-00/CP power supply provides 5 VDC @4 A and 12VDC @ 0.5 A from an input of 90 – 250 VAC, 44 – 440 Hz. The 5-volt out put is adjusted to 5.2 VDC for normal system operation and the 12-volt output provides power to charge the battery. The battery is an 8-volt, 3-ampeare-hour, lead-acid battery manufactured by Sonnenschein (model A208/3S).

A Power Supply board, AC6002, monitors external power, maintains the battery charge, and switches the battery output to the controller circuitry in the event of a power failure. This is a custom designed board located on the right side of the chassis on the top panel. The adjustment procedure for this circuit board and the power supply is found in the Maintenance Procedures, Section 3.6.

2.2 Microprocessor Board

The heart of the Authentication Controller is a Basicon MC-2N programmable controller located at the right, rear corner of the chassis. This unit is a commercial component, but has been slightly customized to allow the microprocessor to address the 500K-byte NOVRAM memory module. An address decoder was provided by Basicon for this purpose and three additional address lines have been attached to the decoder chip socket U4 since there are no header connections available for this purpose in the board design. Drawings AC5000 and AC5100 show details of these connections.
The microprocessor board is configured for a specific application by installing jumpers at locations shown in Figure 2. Jumpers are installed in the positions that are indicated by IN. Jumper positions designated as OUT in the Table 1 are left open.

The embedded software that operates each Authentication Controller resides on a 64K 27C512 EPROM that is labeled with the software version number. The EPROM socket is located on the microprocessor board and is easily accessible.

2.3 I/O Expander Board

A Basicon Input /Output Expander board, model ION-1, is mounted directory under the microprocessor board. The ION-1 board expands the I/O capabilities of the system and permits several isolated I/O boards to be addressed by the system.

2.4 Isolated I/O Boards

In order to isolate the authentication equipment from the FCA AC/S equipment, Basicon IIO boards are used to optically isolate sensor inputs to the authentication equipment and to relay isolate all outputs to the AC/S system. The IIO boards are located at the left side of the chassis.

2.5 Clock Interface Board

Time and date information from the FCA AC/S system is presented to the authentication equipment on 31 inputs. These inputs must be optically isolated and decoded so that the desired data can be selected and put on a parallel bus when it is needed. Since this application is unique, the Clock Interface is a custom designed board that provides optical isolation and decoding functions.

The Clock Interface board, AC6001, is located near the front center of the chassis directory over the DataKey Interface board. The clock interface inputs to the board are provided through two connectors on the back edge of the board.

2.6 DataKey Interface Board

This printed circuit board, mounted directory under the Clock Interface board, is essentially the internal components taken from a model SKS – 232A DataKey Interface Module. It has been slightly modified to operate directly from the 5 VDC power supply, but is otherwise unchanged. Communication between the DataKey Interface and the microprocessor is done through the RS232 channel 0 of the Basicon MC – 2N board.

2.7 DataKey Interface Module

To program the DataKeys, the user needs a personal computer using the PROGDKEY software and a DataKey model SKS – 232A Interface Module. The

Interface Module has an AC power adapter that will operate from 100 – 120 VAC at 50 – 60 Hz. The power adapter cord and an RS232 cable from the computer plug into connectors on the rear of the Interface Module. The module will accept 1K, 2K and 4K serial DataKeys, and any of those keys can be used with the authentication equipment. The DataKeys originally supplied with the system were DK1000 1K serial DataKeys.

2.8 Communication

The RS232 communication protocols associated with the system are listed below. The system software (ONSITE and PROGDKEY) set the computer COM1 serial port to the required parameters.

Authentication Controller Protocols:

- 19200 baud, 8 data bits, 1 stop bit, no parity
- DTR, RTS, and DSR lines are connected at the Authentication Controller end to allow the computer to verify that communications are established.
- Communication cable details are provided in the Operator's Manual and are shown below:

Computer COM 1 **(DE-9S conn.)**		**Auth. Controller** **(DB-25P conn.)**
3	Receive data	2
2	Transmit data	3
7	Request to send	4
8	Clear to send	5
6	Data set ready	6
5	Signal ground	7
4	Data term. Ready	20

DataKey Interface Module Protocols:

- 1200 baud, 8 data bits, 1 start bit, 1 stop bit, odd parity
- The communication cable should be a straight- through RS232 cable with the following minimum connections:

Computer COM 1		**DataKey Interface (DB-25P conn.)**
1	Protective gnd	1
2	Transmit data	2
3	Receive data	3
4	Request to send	4
5	Clear to send	5
7	Signal ground	7

It may be necessary to use a 9-pin to 25-pin adapter with the cable described above to mate to the computer RS232 connector.

3. Maintenance Procedures

3.1 Remove Power

The Authentication Equipment is normally powered externally from facility power and operates from 90 – 250 VAC at 44 – 440 Hz. An internal battery provides up to three hours of backup power in the event of a loss of facility power. When performing maintenance procedures on the Authentication Controllers, both power sources should be disabled.

Procedure

1. To access the interior of the Authentication Controller, remove the four large nuts that secure the enclosure cover and lift it off.
2. Remove the AC power from the controller by unplugging the power cable from connector J4, located near the front of the chassis.
3. Disable the DC power by removing the 3A fuse, F1, from the Power Supply Board which is vertically mounted on the right side of the chassis. To remove F1, pull the fuse straight out of the socket. To prevent misplacing the fuse, insert it offset in the socket with only one pin engaged. When the AC and DC power have been disabled, further disassembly can be safely performed.
4. To verify that the power has been disabled, check the voltage between the 5-volt and ground buses located adjacent to the Power Supply Board. The 5-volt bus should be at a ground potential if the procedure has been done

correctly.

3.2 Replace NOVRAM Cartridge

With the enclosure cover removed, the NOVRAM cartridge is visible near the rear center of chassis. The cartridge is a Dallas Semiconductor DS1217M4-25 Nonvolatile Read/Write Cartridge. The cartridge is manufactured with an internal battery that has an expected life of five years from the date of manufacture. The manufacture date code is on the back of the cartridge in a four digit format in the form of AABB where AA designates the year of manufacture and BB designates the week of manufacture.

Procedure

1. To replace the cartridge, pull it out of the socket and insert a replacement.
2. After replacing the NOVRAM cartridge, perform a self test on the Authentication Controller before beginning an acquisition period.

3.3 Replace EPROM

If it is necessary to upgrade the embedded software in a Authentication Controller, the EPROM on the MC-2N Microprocessor Board must be replaced. The system power should be removed as described in Section 3.1 before replacing the EPROM. The EPROM socket is the one nearest to the center of chassis, but since there is only one 28-pin EPROM on the Microprocessor board, the socket should be easy to identify. If correct polarity is observed and care is taken to avoid damage to the EPROM pins during removal and insertion, there should be little difficulty in replacing this part. When the procedure is completed, restore power to the Authentication Controller.

3.4 Remove chassis from Enclosure

When power has been removed from the Authentication Controller, the chassis can be removed from the protective enclosure. If the AC power cable has already been removed, there are four remaining signal cables that must be disconnected.

Procedure

1. At the rear of chassis, unplug the two 50-pin connectors. Take care NOT to pull on the wires that are connected to the nearby orange connectors.
2. The remaining two cables are connected to the Clock Interface Board and are located on the top, center of the chassis. Unplug these two connectors carefully to avoid damage to the header pins.
3. At the extreme left side of the PN/M Authentication Controller chassis a 10-pin connector is visible on the upper I/O board. Unplug this connector to allow adequate clearance for the chassis when it is lifted out of the enclosure.
4. The RS232 connector bracket is secured to the chassis by two Phillips head screws. Loosen these two screws and slide the bracket back from the front panel of the enclosure. If it will not remain in this position tighten one of the screws enough to hold it away from the front panel.
5. Near each of the four corners of the chassis there is a Knurled Knob that secures the chassis to the bottom of the enclosure. Unscrew and remove these four knobs to permit removal of the chassis. There is limited clearance and if this procedure is being conducted with gloves on, it requires dexterity and strength of character. Take care not to bend the header pins at the left side of the chassis, especially if gloves are being worn because they readily snag these pins. When all four Knobs are removed the chassis is free from the enclosure.
6. To remove the chassis from the enclosure, grasp the upper plate of the chassis near the center and lift the chassis up to clear the threaded studs at the corners. Tilt the right side of the chassis up while keeping the left side of the chassis against the lower, left side of the enclosure. The right side of the chassis should clear the brackets on the upper, right side of the enclosure and then the entire chassis can be lifted out of the enclosure. The chassis should be set on a flat surface before proceeding further.

3.5 Battery Replacement

Procedure

1. Remove the chassis from the enclosure according to the procedure described in Section 3.4. The battery is located on the right rear of the chassis on the lower panel. The battery is an 8-volt, 3-ampeare- hour, lead-acid battery

which has an expected life of five years.

2. Take note of the polarity of the battery connectors.
3. Pull the battery connectors off of the battery terminals before removing the battery.
4. A bracket secures the battery to the chassis and the four bracket mounting screws are accessible from the bottom of the chassis. These screws need only be loosened to remove or replace the battery. When the bracket is loosened, the battery will slide out the right side of the chassis.
5. Insert a replacement battery in the battery holder bracket in the same orientation as the battery that was removed.
6. Tighten the four bracket mounting screws to secure the battery, and reconnect the two battery connectors with the correct polarity.
7. Verify the correct polarity of the connections by measuring the positive battery voltage from the ground bus to BAT terminal near the fuse, F1, on the Power Supply Board.

3.6 Power Supply Adjustment

There are several adjustments that should be made on the power supply module and on the Power Supply board AC6002 if replacements of these units is required. Basicon recommends that their equipment be operated at 5.2 VDC so the power supply must be adjusted to this value. The Power Supply board has two adjustments that set the switching threshold for the power failure detection and the battery charging voltage.

This procedure requires access to the power supply voltage adjustment so the chassis should be removed from the enclosure and AC line voltage has to be provided to the power supply.

The power supply voltage output is set by adjusting a potentiometer that is visible at the right side of the power supply module between the two connector blocks. Adjustments to the Power Supply board AC6002 are made to R4 and R2 which are accessible at the top edge of the board. Two voltmeters are required for this procedure and one of these should be a recently calibrated digital meter.

Procedure

1. Disconnect J1of the Microprocessor board.
2. Use the calibrated voltmeter to monitor the voltage at the 5V bus with respect to the ground bus.

3. With the other voltmeter, monitor the voltage at the AC ON terminal adjacent to R4 on the Power Supply board.
4. Replace the fuse F1 in the fuse holder and apply AC power. The AC ON terminal should be at approximately 5VAC when power is applied.
5. Carefully adjust the power supply output to between 5.15 VDC and 5.20 VDC as measured at the 5V bus by adjusting the potentiometer on the power supply module.
6. Set the switching threshold to 5.15 VDC by adjusting R4, located near the front of the Power Supply board. While monitoring the AC ON voltage, carefully lower the power supply voltage through 5.15 VDC. If the AC ON voltage does not change at 5.15 VDC, adjust R4 until it does. Then repeat the process to check the threshold. The goal is to have the transition from a logical high to a logical low occur at AC ON when the power supply voltage drops to 5.15 VDC. The procedure may have to be repeated several times until the threshold can be set to 5.15 VDC.
7. Disconnect the positive battery connector and continue to monitor the voltage at the 5V bus. Adjust the power supply output to 5.20 VDC. Then connected the calibrated voltmeter to positive battery wire (it is still disconnected from the battery) and adjust R1 on the Power Supply board for a 9.20 VDC reading. Recheck the 5V bus for a 5.20 VDC reading and then reconnect the battery terminal to the battery. Depending on the charge state of the battery the 5V bus voltage may drop slightly, but that is acceptable.

   Note: After these adjustments have been made the system will normally operate at 5.2 VDC and the battery will "float" at 9.2 VDC. In the event of a power failure, the battery output will be switched into the circuit when the power supply output falls below 5.15 VDC and the system will operate at 5 VDC until AC power is restored. Charging current is limited by the power supply output.
8. Remove the fuse F1 and remove AC power from the unit.
9. Reconnect the battery terminals and J1 on the Microprocessor board.

3.7 Install Chassis in Enclosure

Procedure

1. Before placing the chassis into the enclosure, arrange the signal and power

cables so that the connectors are outside the enclosure.

2. Verify that the four 0.5-inch spacers are in place over the threaded studs in the bottom corners of the enclosure and that the two screws that secure the RS232 connector bracket to the chassis are loosened to permit the bracket to move.
3. Lower the left side of the chassis into the enclosure first to allow the right side to clear the brackets at the upper right side of the enclosure. Remember that the 10-pin connector at the extreme left side of the PN/M Authentication Controller chassis must be removed to provide adequate clearance during this maneuver, and replaced when the chassis is in place.
4. Arrange the signal and power cables to prevent pinching them when the chassis secured, and to allow the connectors to be mated to the chassis connectors.
5. When the four threaded studs at the bottom corners of the enclosure are aligned in the slotted holes in the chassis, slide the chassis forward until the DataKey receptacle is against or very near the front panel of the enclosure.
6. Secure the chassis in the enclosure with the four knurled knobs.
7. Slide the RS232 bracket forward until the connector extends through the enclosure panel, and then secure the bracket by tightening the two Phillips head screws.
8. Connect the four signal cables and the power cable to their mating connectors. The clock interface cables are marked to correspond to the connectors on the Clock Interface board.
9. Insert the fuse, F1, into the fuse holder on the Power Supply board and verify that any connectors that were removed have been reconnected.
10. Replace and secure the enclosure cover.

Table 1 Jumper Installation

E1	OUT	E9	OUT	E17	IN
E2	OUT	E10	OUT	E18	OUT
E3	OUT	E11	IN	E19	OUT
E4	OUT	E12	OUT	E20	IN
E5	OUT	E13	IN	E21	OUT
E6	OUT	E14	OUT	E22	IN
E7	OUT	E15	IN	E23	IN
E8	OUT	E16	OUT	E24	OUT

Jumper Table

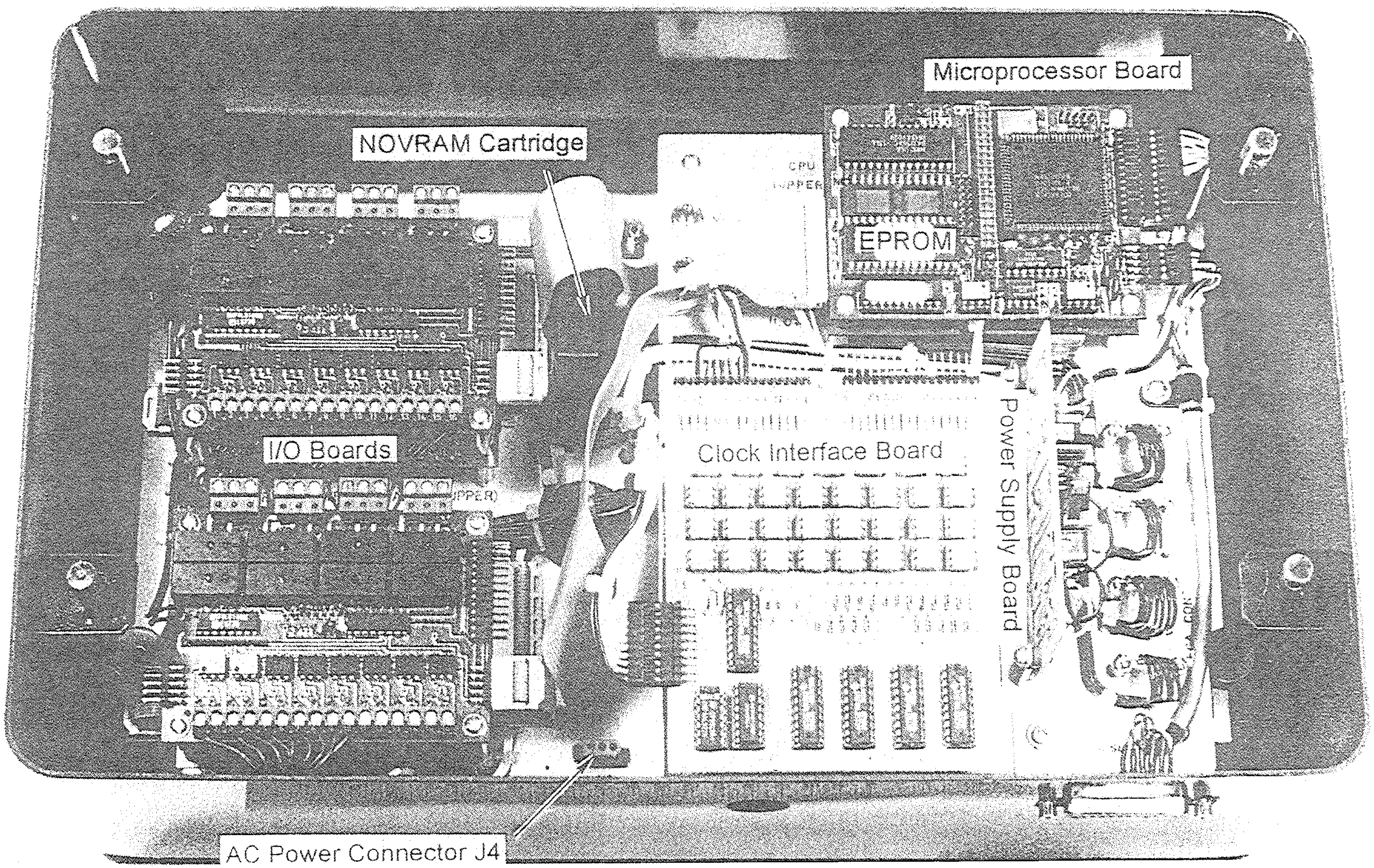


Figure 1 P/M Authentication Controller with cover removed

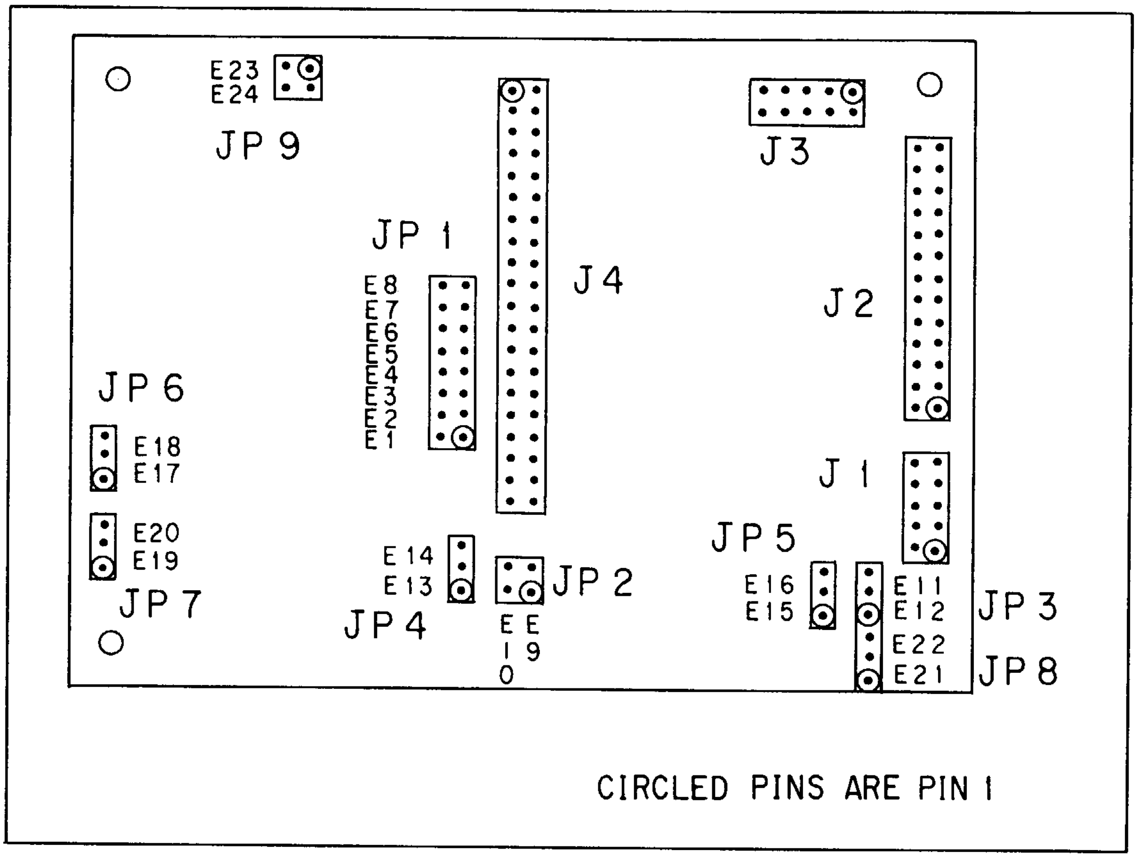
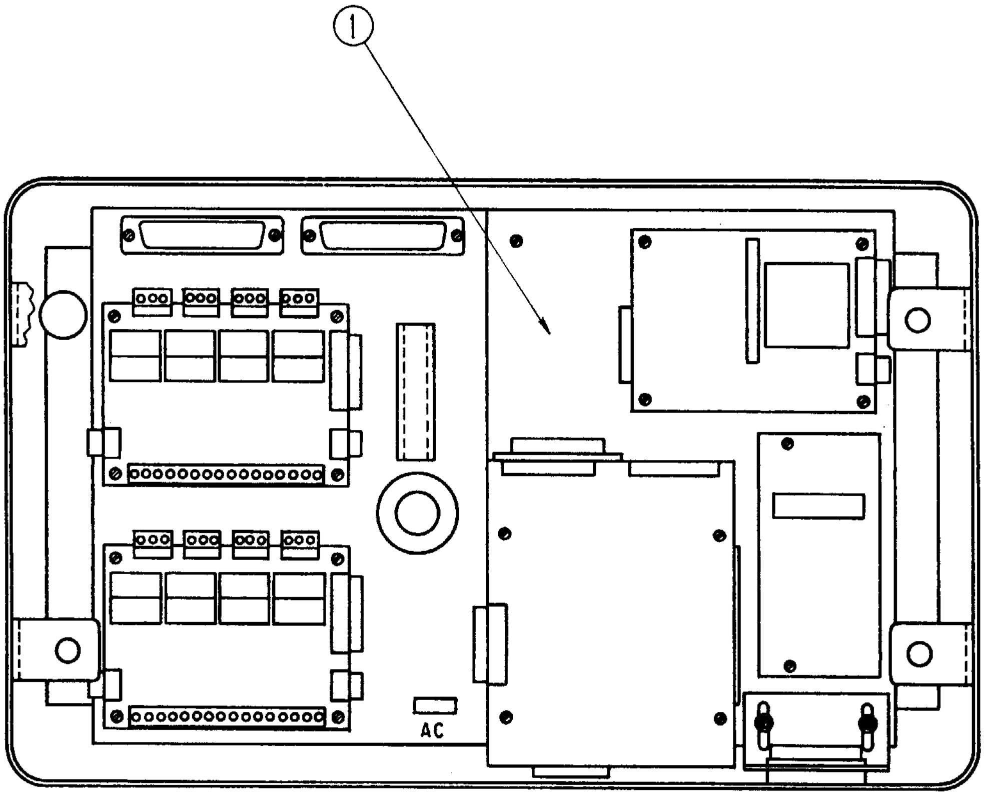
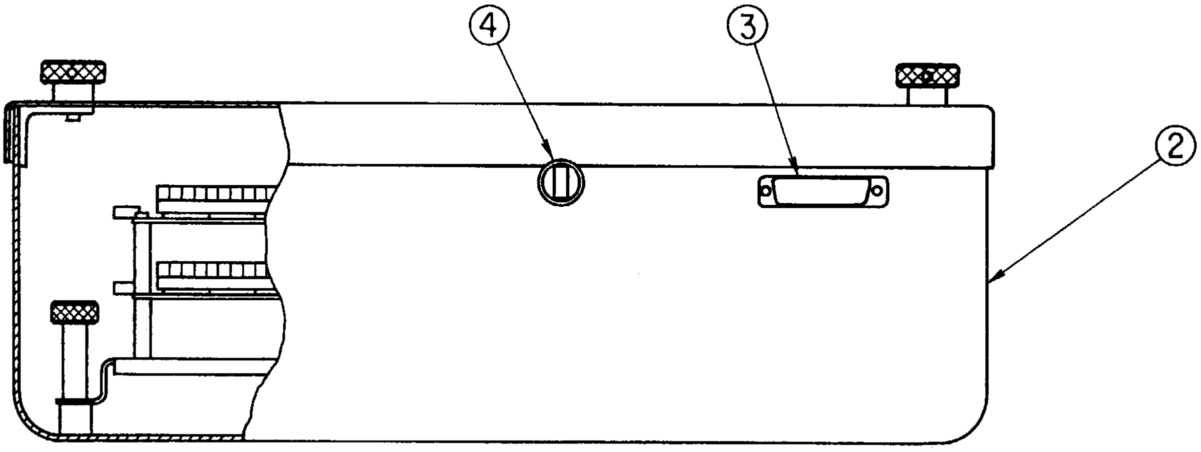


Figure 2. MC-2N Jumper and Connector Locations

Drawings

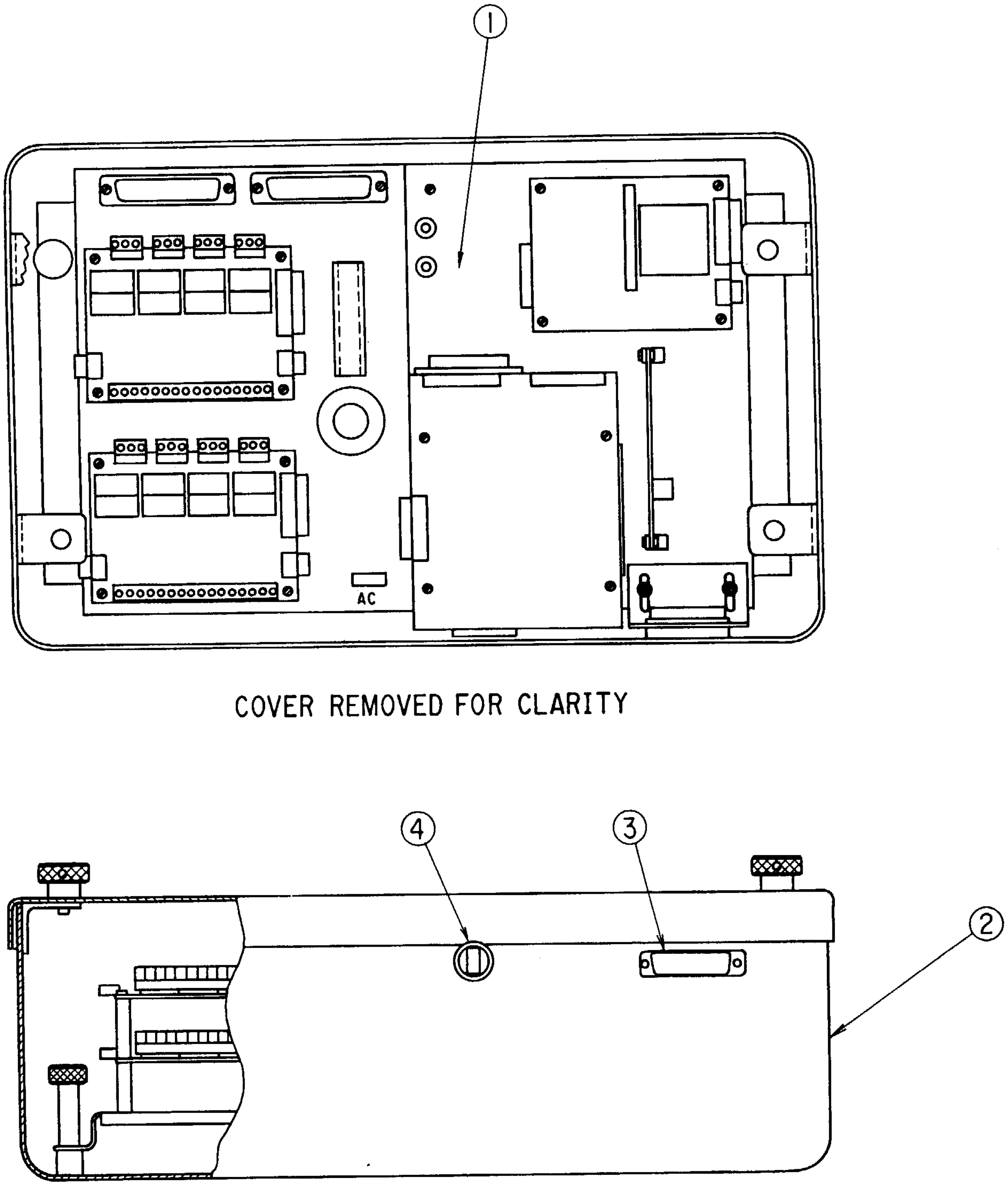


COVER REMOVED FOR CLARITY



① Sub-Assembly of Authentication
② Housing of Authentication Controller
③ Connector for RS232 Communication
④ DataKey Socket

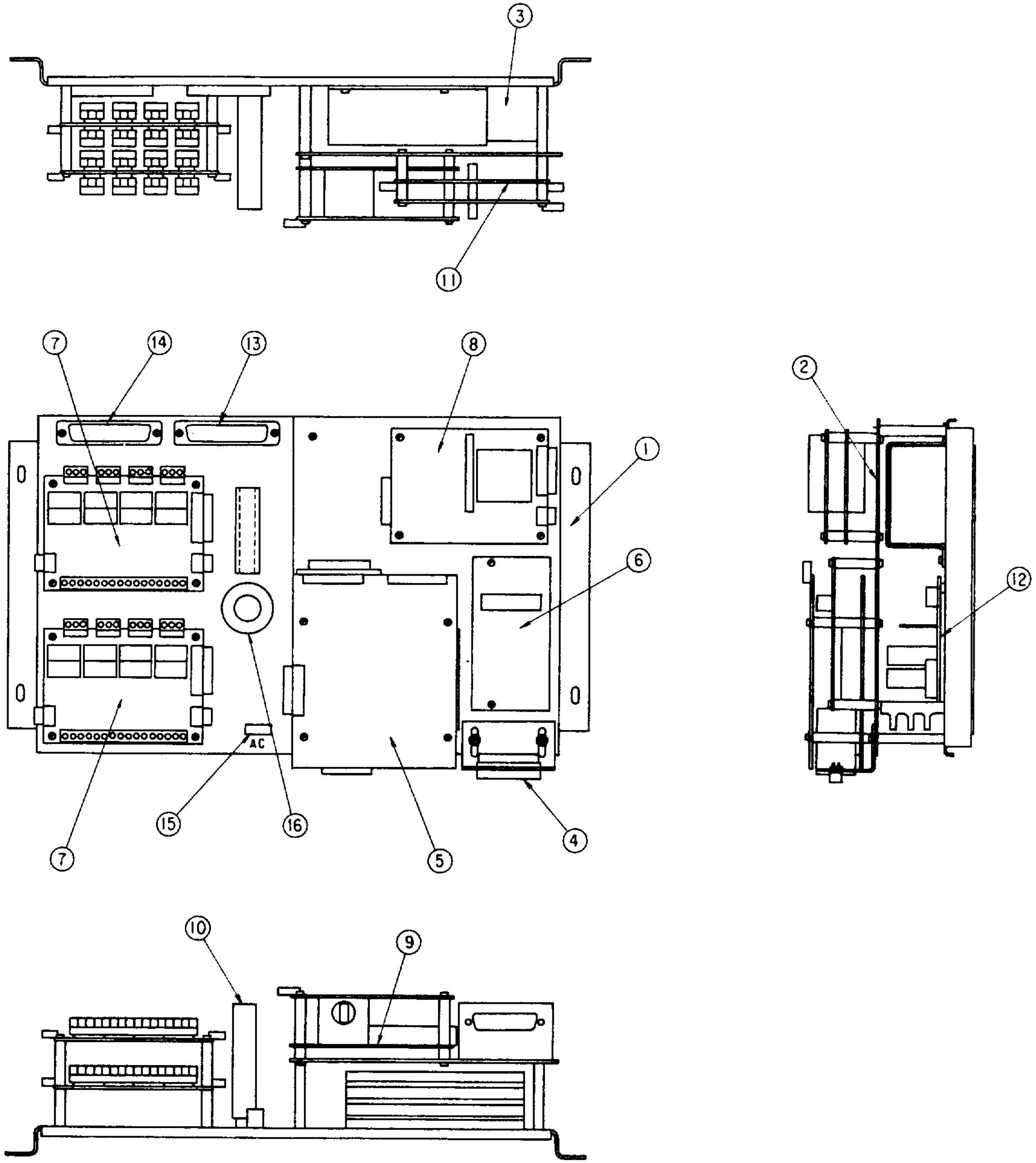
PN/M AUTHENTICATION CONTROLLER : AC1000



COVER REMOVED FOR CLARITY

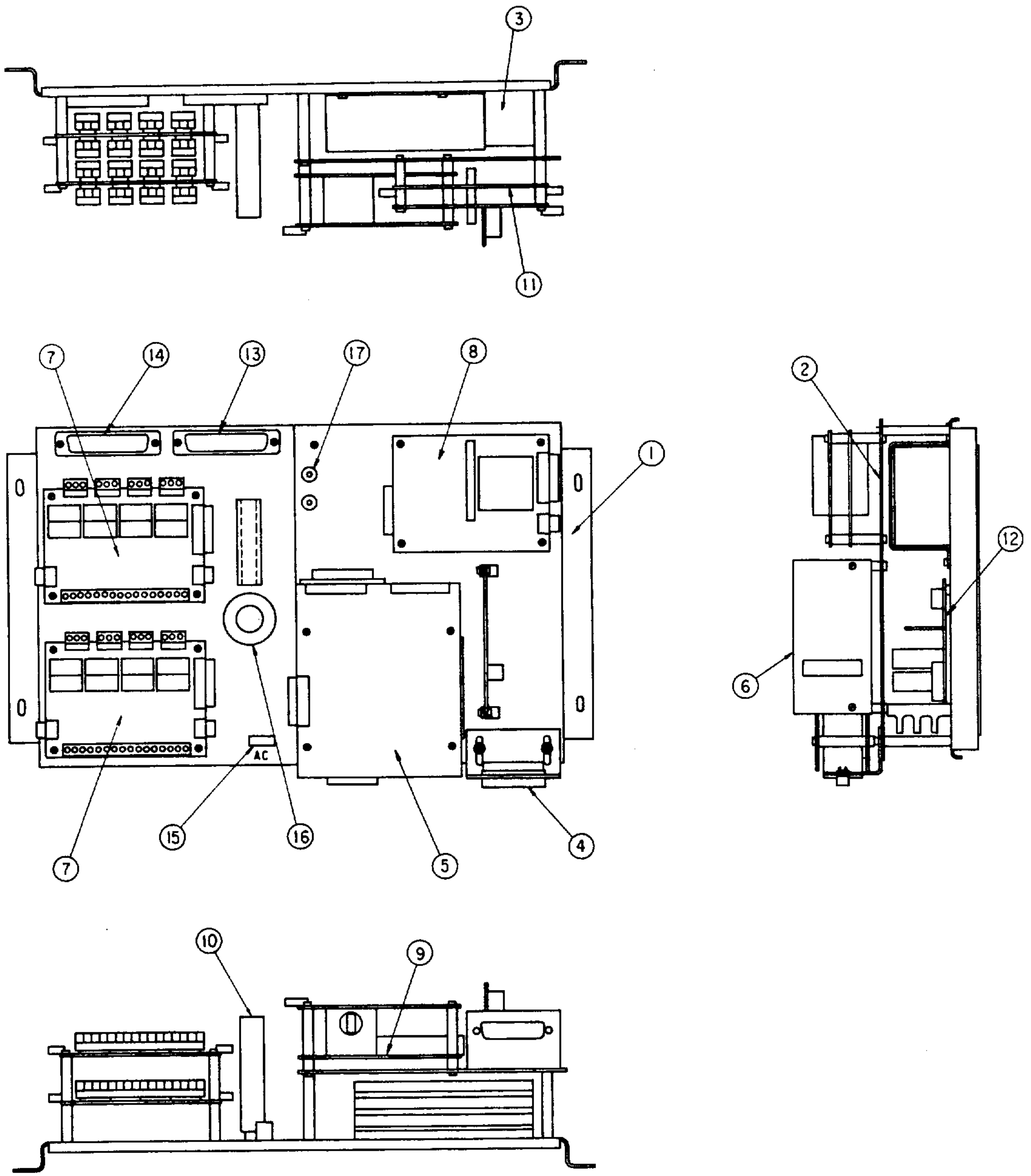
① Sub-Assembly of Authentication
② Housing of Authentication Controller
③ Connector for RS232 Communication
④ DataKey Socket

P/M AUTHENTICATION CONTROLLER : AC1100



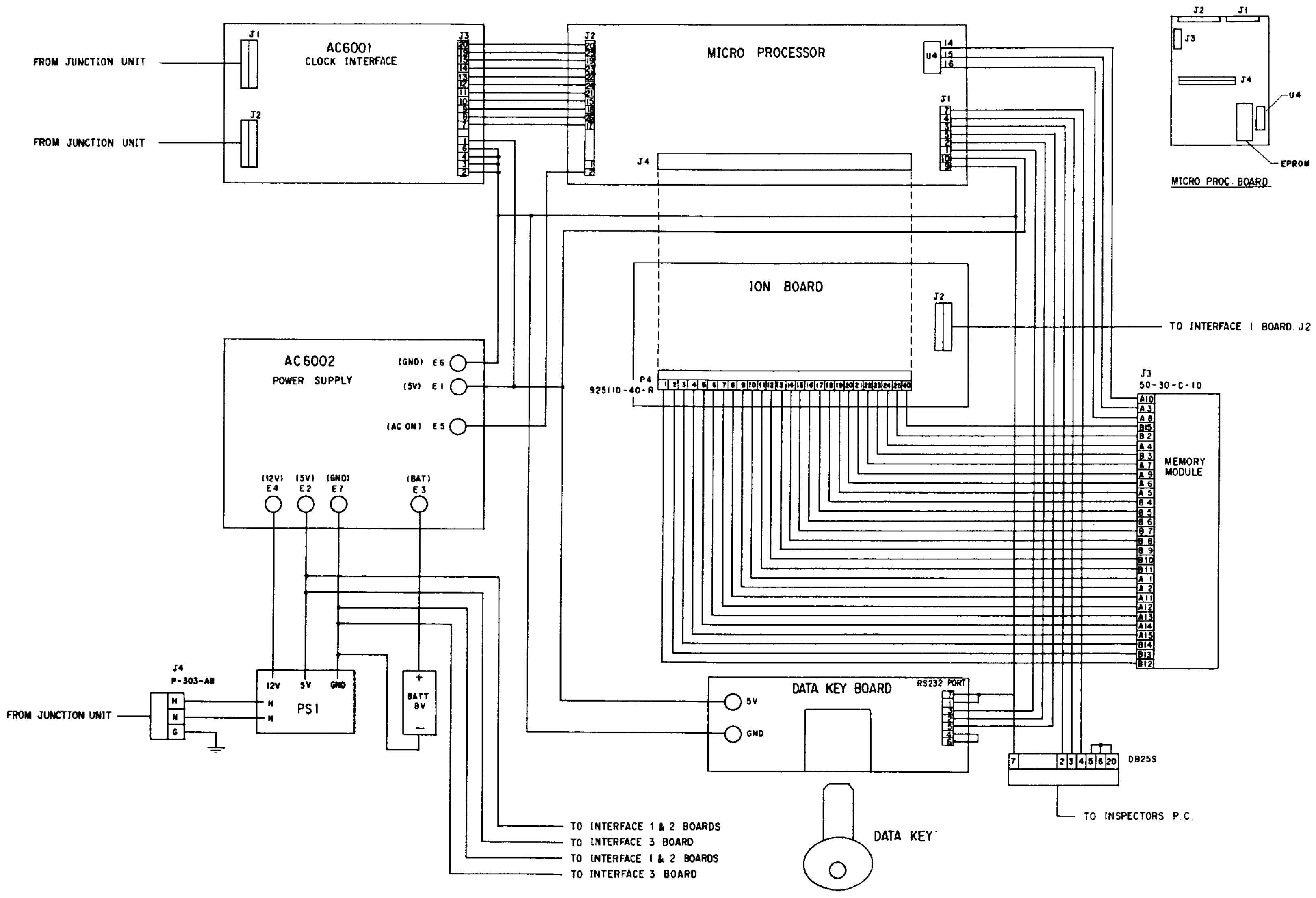
① Base Plate
② Mount Plate
③ Battery
④ Connector, DB-25S
⑤ Clock Interface
⑥ Controller, Power Supply
⑦ Input-Output Interface Board
⑧ ION Board
⑨ DataKey Board
⑩ Memory Module
⑪ Microprocessor Board
⑫ Power Supply
⑬ Connector, DD-50-P
⑭ Connector, DD-50-S
⑮ Connector for AC Power
⑯ Rubber Grommet

SUB-ASSEMBLY : AC2100
PN/M AUTHENTICATION CONTROLLER

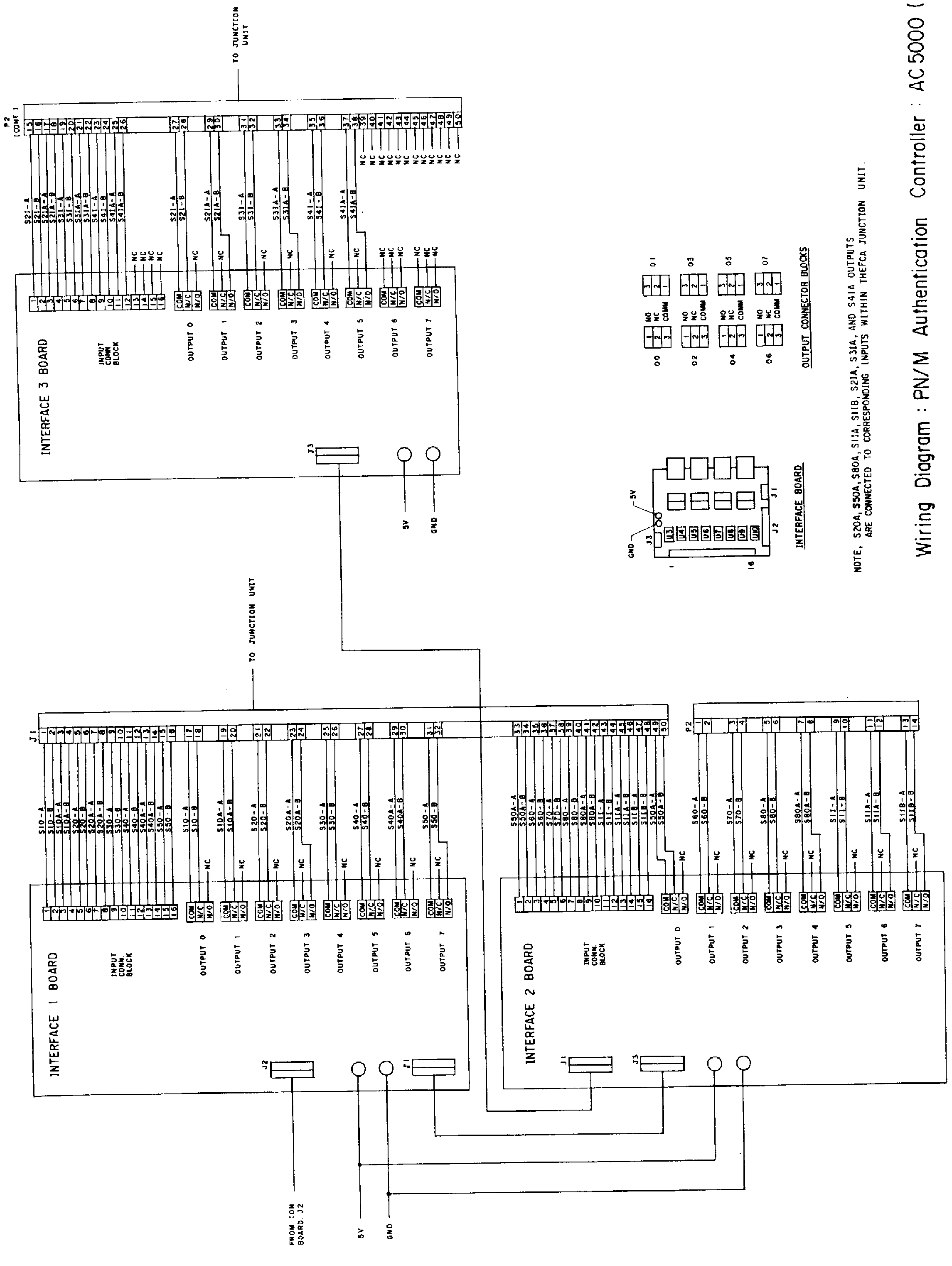


① Base Plate
② Mount Plate
③ Battery
④ Connector, DB-25S
⑤ Clock Interface
⑥ Controller, Power Supply
⑦ Input-Output Interface Board
⑧ ION Board
⑨ DataKey Board
⑩ Memory Module
⑪ Microprocessor Board
⑫ Power Supply
⑬ Connector, DD-50-P
⑭ Connector, DD-50-S
⑮ Connector for AC Power
⑯ Rubber Grommet
⑰ Momentary Switch for MD1

SUB-ASSEMBLY : AC2200
P/M AUTHENTICATION CONTROLLER

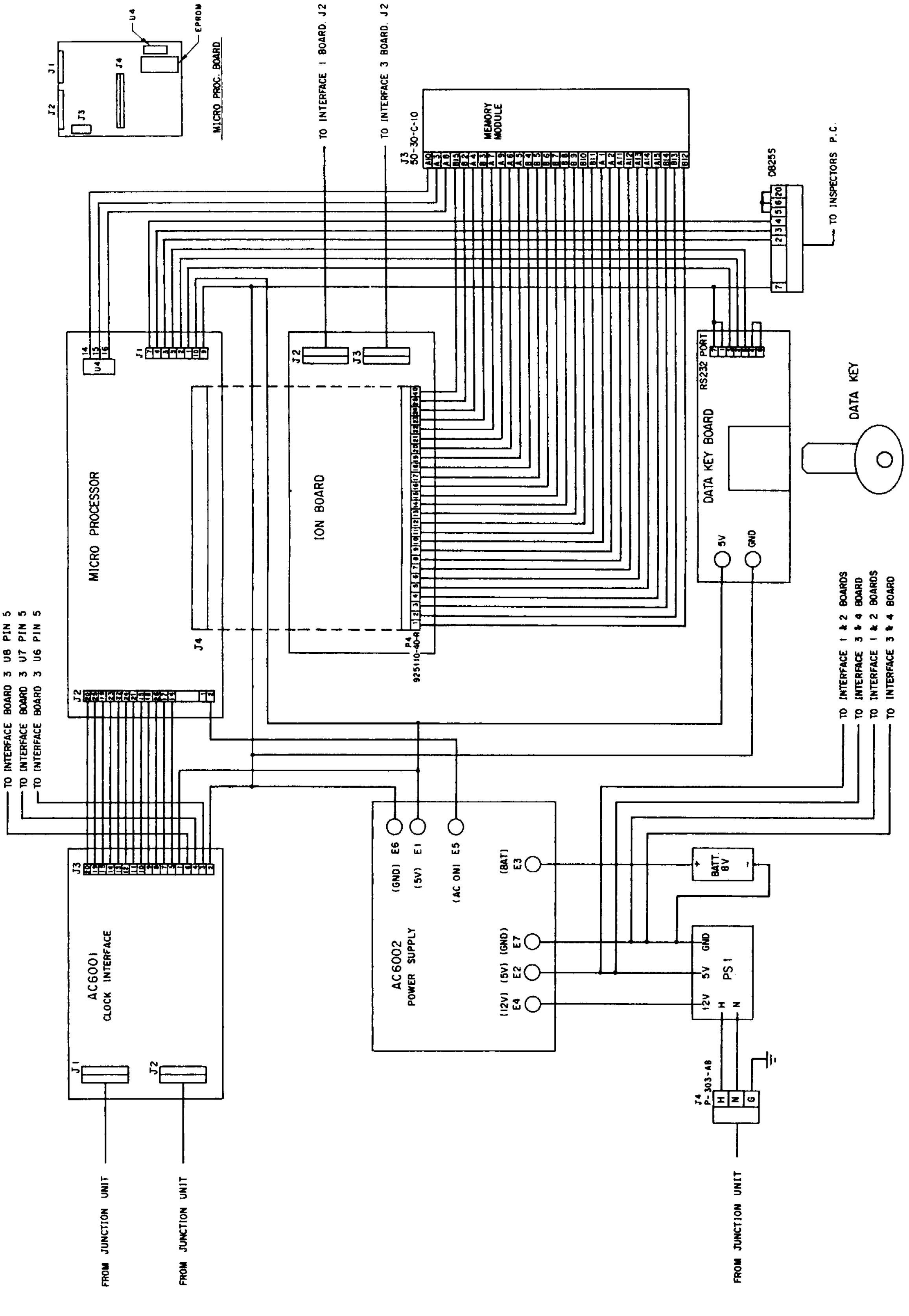


Wiring Diagram : PN/M Authentication Controller : AC5000 (1 of 2)

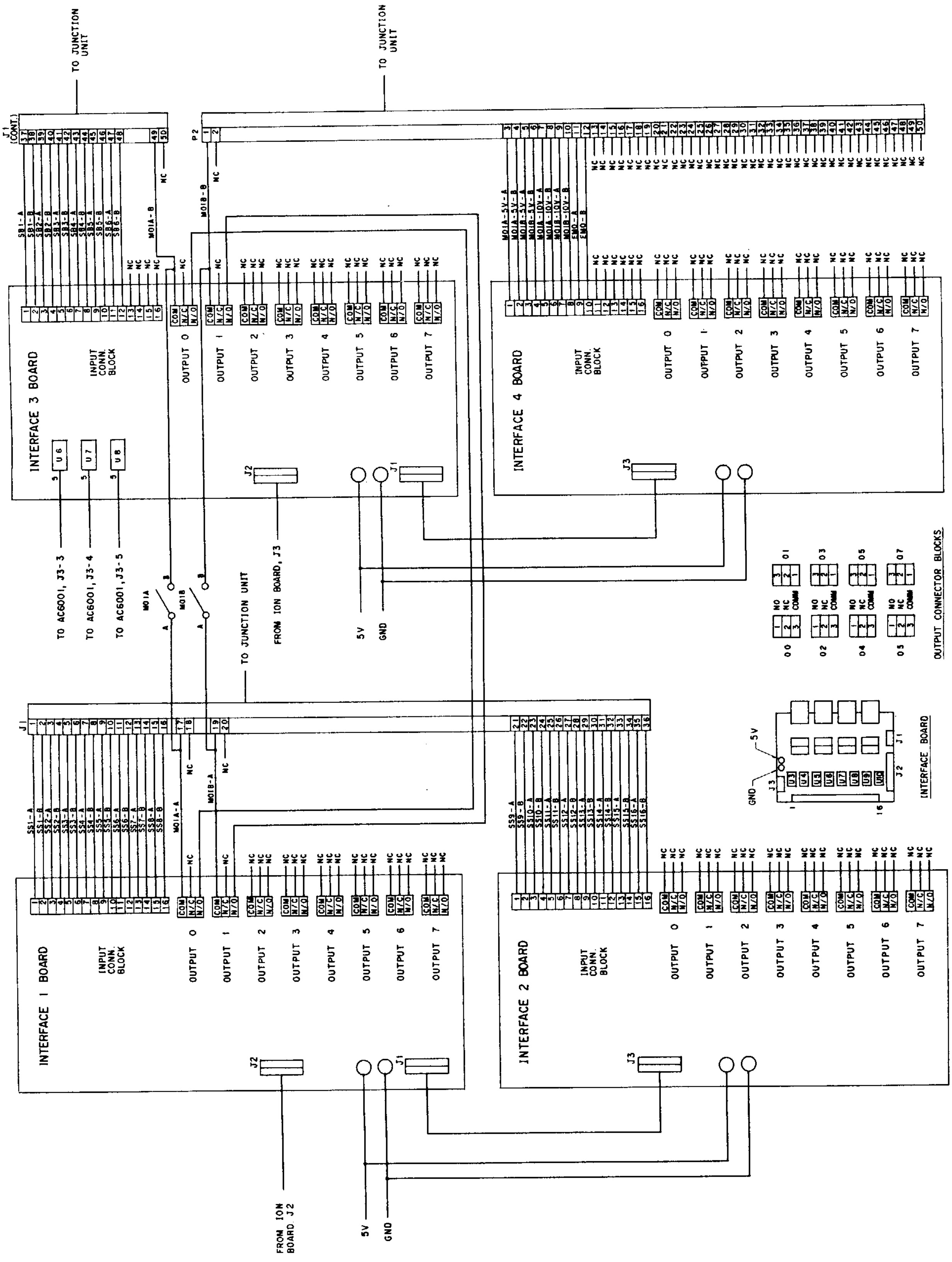


NOTE, S20A, S50A, S80A, S11A, S11B, S21A, S31A, AND S41A OUTPUTS ARE CONNECTED TO CORRESPONDING INPUTS WITHIN THEFCA JUNCTION UNIT.

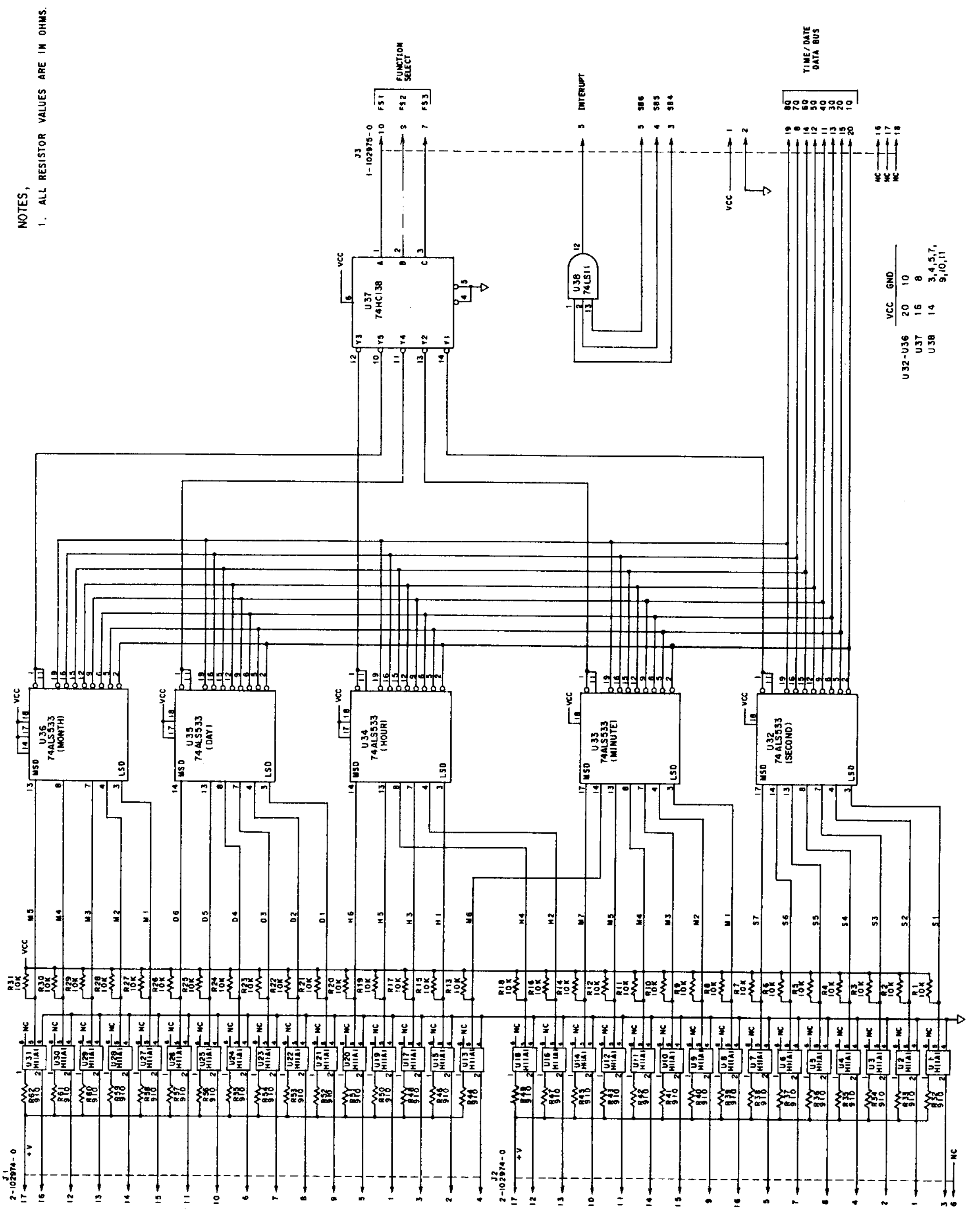
Wiring Diagram : PN/M Authentication Controller : AC5000 (2 of 2)



Wiring Diagram : P/M Authentication Controller : AC5100 (1 of 2)



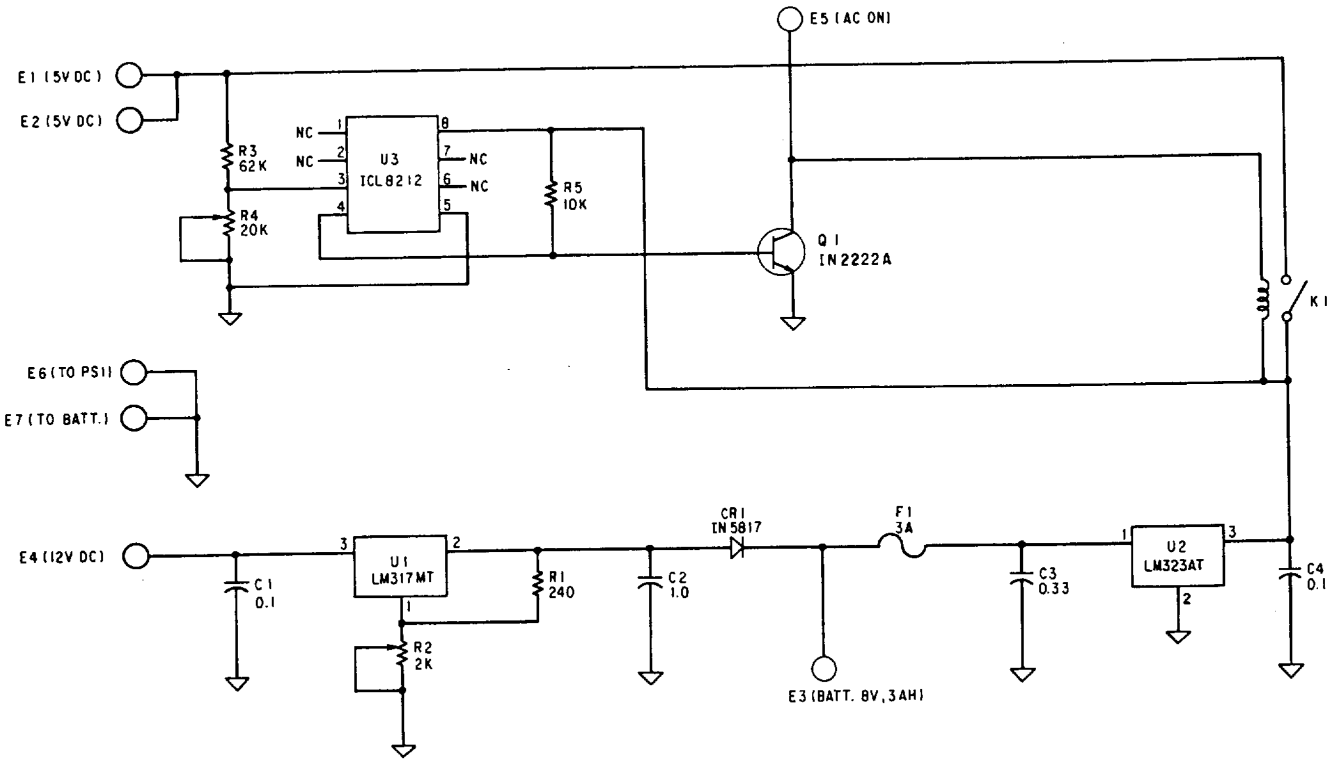
Wiring Diagram : P/M Authentication Controller : AC5100 (2 of 2)



Wiring Diagram : Clock Interface .Board : AC6001 (1 of 1)

NOTES:

1. ALL RESISTOR VALUES ARE IN OHMS.
2. ALL CAPACITOR VALUES ARE IN MICROFARADS.
3. ADJUST 5V POWER SUPPLY TO 5.2V.
4. ADJUST R4 FOR 5.15 VDC THRESHOLD.
5. ADJUST R2 FOR 9.2 VDC AT BATTERY.



Wiring Diagram : Power Supply Board : AC6002 (1 of 1)

国際単位系 (SI) と換算表

表1　SI基本単位および補助単位

量	名称	記号
長さ	メートル	m
質量	キログラム	kg
時間	秒	s
電流	アンペア	A
熱力学温度	ケルビン	K
物質量	モル	mol
光度	カンデラ	cd
平面角	ラジアン	rad
立体角	ステラジアン	sr

表3　固有の名称をもつSI組立単位

量	名称	記号	他のSI単位による表現
周波数	ヘルツ	Hz	s^{-1}
力	ニュートン	N	$m\cdot kg/s^2$
圧力，応力	パスカル	Pa	N/m^2
エネルギー，仕事，熱量	ジュール	J	N·m
工率，放射束	ワット	W	J/s
電気量，電荷	クーロン	C	A·s
電位，電圧，起電力	ボルト	V	W/A
静電容量	ファラド	F	C/V
電気抵抗	オーム	Ω	V/A
コンダクタンス	ジーメンス	S	A/V
磁束	ウェーバ	Wb	V·s
磁束密度	テスラ	T	Wb/m^2
インダクタンス	ヘンリー	H	Wb/A
セルシウス温度	セルシウス度	℃	
光束	ルーメン	lm	cd·sr
照度	ルクス	lx	lm/m^2
放射能	ベクレル	Bq	s^{-1}
吸収線量	グレイ	Gy	J/kg
線量当量	シーベルト	Sv	J/kg

表2　SIと併用される単位

名称	記号
分，時，日	min, h, d
度，分，秒	°, ′, ″
リットル	l, L
トン	t
電子ボルト	eV
原子質量単位	u

$1\ eV = 1.60218 \times 10^{-19}\ J$

$1\ u = 1.66054 \times 10^{-27}\ kg$

表4　SIと共に暫定的に維持される単位

名称	記号
オングストローム	Å
バーン	b
バール	bar
ガル	Gal
キュリー	Ci
レントゲン	R
ラド	rad
レム	rem

$1\ Å = 0.1\ nm = 10^{-10}\ m$

$1\ b = 100\ fm^2 = 10^{-28}\ m^2$

$1\ bar = 0.1\ MPa = 10^5\ Pa$

$1\ Gal = 1\ cm/s^2 = 10^{-2}\ m/s^2$

$1\ Ci = 3.7 \times 10^{10}\ Bq$

$1\ R = 2.58 \times 10^{-4}\ C/kg$

$1\ rad = 1\ cGy = 10^{-2}\ Gy$

$1\ rem = 1\ cSv = 10\ ^{2}\ Sv$

表5　SI接頭語

倍数	接頭語	記号
10^{18}	エクサ	E
10^{15}	ペタ	P
10^{12}	テラ	T
10^{9}	ギガ	G
10^{6}	メガ	M
10^{3}	キロ	k
10^{2}	ヘクト	h
10^{1}	デカ	da
10^{-1}	デシ	d
10^{-2}	センチ	c
10^{-3}	ミリ	m
10^{-6}	マイクロ	μ
10^{-9}	ナノ	n
10^{-12}	ピコ	p
10^{-15}	フェムト	f
10^{-18}	アト	a

（注）

1. 表1－5は「国際単位系」第5版，国際度量衡局 1985年刊行による。ただし，1 eV および1 u の値はCODATA の1986年推奨値によった。
2. 表4には海里，ノット，アール，ヘクタールも含まれているが日常の単位なのでここでは省略した。
3. barは，JISでは流体の圧力を表わす場合に限り表2のカテゴリーに分類されている。
4. EC閣僚理事会指令ではbar，barnおよび「血圧の単位」mmHgを表2のカテゴリーに入れている。

換　算　表

力	$N (=10^5 dyn)$	kgf	lbf
	1	0.101972	0.224809
	9.80665	1	2.20462
	4.44822	0.453592	1

粘　度　$1\ Pa\cdot s (N\cdot s/m^2) = 10\ P$（ポアズ）$(g/(cm\cdot s))$

動粘度　$1\ m^2/s = 10^4\ St$（ストークス）(cm^2/s)

圧力	MPa(=10 bar)	kgf/cm^2	atm	mmHg(Torr)	lbf/in^2(psi)
	1	10.1972	9.86923	7.50062×10^3	145.038
	0.0980665	1	0.967841	735.559	14.2233
	0.101325	1.03323	1	760	14.6959
	1.33322×10^{-4}	1.35951×10^{-3}	1.31579×10^{-3}	1	1.93368×10^{-2}
	6.89476×10^{-3}	7.03070×10^{-2}	6.80460×10^{-2}	51.7149	1

エネルギー・仕事・熱量	$J (=10^7 erg)$	kgf・m	kW・h	cal（計量法）	Btu	ft・lbf	eV
	1	0.101972	2.77778×10^{-7}	0.238889	9.47813×10^{-4}	0.737562	6.24150×10^{18}
	9.80665	1	2.72407×10^{-6}	2.34270	9.29487×10^{-3}	7.23301	6.12082×10^{19}
	3.6×10^6	3.67098×10^5	1	8.59999×10^5	3412.13	2.65522×10^6	2.24694×10^{25}
	4.18605	0.426858	1.16279×10^{-6}	1	3.96759×10^{-3}	3.08747	2.61272×10^{19}
	1055.06	107.586	2.93072×10^{-4}	252.042	1	778.172	6.58515×10^{21}
	1.35582	0.138255	3.76616×10^{-7}	0.323890	1.28506×10^{-3}	1	8.46233×10^{18}
	1.60218×10^{-19}	1.63377×10^{-20}	4.45050×10^{-26}	3.82743×10^{-20}	1.51857×10^{-22}	1.18171×10^{-19}	1

1 cal = 4.18605 J（計量法）
　= 4.184 J　（熱化学）
　= 4.1855 J　(15 °C)
　= 4.1868 J（国際蒸気表）

仕事率　1 PS（仏馬力）
　= 75 kgf·m/s
　= 735.499 W

放射能	Bq	Ci
	1	2.70270×10^{-11}
	3.7×10^{10}	1

吸収線量	Gy	rad
	1	100
	0.01	1

照射線量	C/kg	R
	1	3876
	2.58×10^{-4}	1

線量当量	Sv	rem
	1	100
	0.01	1

（86年12月26日現在）

DEVELOPMENT OF AUTHENTICATION SYSTEM FOR THE FAST CRITICAL ASSEMBLY (FCA) PORTAL MONITOR (P/M) AND PENETRATION MONITOR (PN/M) SYSTEMS OF JAERI