JAERI-M
92-026

JASPAS 91-2

UPGRADED RECOVER SYSTEM

— CASDAC SYSTEM —

March 1992

Yoichi YAMAMOTO and Kinji KOYAMA

日 本 原 子 力 研 究 所
Japan Atomic Energy Research Institute

JAERI-M
92-026

JASPAS 91-2

UPGRADED RECOVER SYSTEM

— CASDAC SYSTEM —

March 1992

Yoichi YAMAMOTO and Kinji KOYAMA

日 本 原 子 力 研 究 所
Japan Atomic Energy Research Institute

JAERI-M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，日本原子力研究所技術情報部情報資料課（〒319-11 茨城県那珂郡東海村）あて，お申しこみください。なお，このほかに財団法人原子力弘済会資料センター（〒319-11 茨城県那珂郡東海村日本原子力研究所内）で複写による実費領布をおこなっております。

JAERI-M reports are issued irregularly.
Inquiries about availability of the reports should be addressed to Information Division Department of Technical Information, Japan Atomic Energy Research Institute, Tokaimura, Naka-gun, Ibaraki-ken 319-11, Japan.

編集兼発行　日本原子力研究所
印　　刷　ニッセイエブロ株式会社

JAERI-M 92-026

Upgraded RECOVER System
- CASDAC System -

Yoichi YAMAMOTO and Kinji KOYAMA

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

(Received January 31, 1992)

The CASDAC (Containment And Surveillance Data Authenticated Communication) system has been developed by JAERI for nuclear safeguards and physical protection of nuclear material. This system was designed and constructed as an upgraded RECOVER system, design concept of which was based on the original RECOVER system and also the TRANSEAVER system. Both of them were developed several years ago as a remote monitoring system for continual verification of security and safeguards status of nuclear material.

The system consists of two subsystems, one of them is a Grand Command Center (GCC) subsystem and the other is a facility subsystem. Communication between two subsystems is controlled through the international telephone line network. Therefore all communication data are encrypted to prevent access by an unauthorized person who may intend to make a falsification, or tapping. The facility subsystem has an appropriate measure that ensure data security and reliable operation under unattended mode of operaton. The software of this system is designed so as to be easily used in other different types of computers.

This report describes the outline of the CASDAC system and the results of its performance tests. This work has been carried out in the framework of Japan Support Programme for Agency Safeguards (JASPAS) as a project, JA-1.

Keywords: CASDAC, RECOVER, TRANSEAVER, Safeguards, Physical Protection, System, C/S (Containment/Surveillance), Verification, Encryption, Communication

JAERI－M 92－026

改良RECOVERシステム
－ CASDACシステム －

日本原子力研究所東海研究所燃料安全工学部
山本 洋一・小山 謹二

（1992年1月31日受理）

CASDAC（封じ込め／監視データ認証通信）システムは，保障措置及び核物質防護の一環として日本原子力研究所が開発した。このシステムはRECOVERシステムとTRANSEAVERシステムを基に，改良RECOVERシステムとして設計，製作された，核物質の保全状況及び保障措置状況の検認を行うための遠隔監視システムである。

本システムは，２つのサブシステムからなり，１つは中央監視センター（GCC），他の１つは施設サブシステムである。両サブシステム間の通信には公衆電話回線網を使用しているため，通信データは非有資格者によるデータ改竄や盗聴を防ぐ目的で暗号化されている。施設サブシステムは無人運転を前提としているので，データ保護対策や動作時の信頼性を高める工夫が施してある。また，システムプログラムは移植性を考慮して作成された。

本報告書は，CASDACシステムの概要及び性能試験について述べたものである。なお，本研究は日本国のIAEA保障措置支援計画の一環としてプロジェクトJA-1として実施したものである。

東海研究所：〒319-11 茨城県那珂郡東海村白方字白根2-4

Contents

目　次

1. Introduction

The CASDAC (Containment and Surveillance Data Authenticated Communication) system has been developed as an upgraded RECOVER system, the system is a secure and reliable data communication system with a function that monitors continually any changes in the status of containment and surveillance sensors and the status of integrity and health of the system itself.

This system is designed and constructed on the basis of the RECOVER [1] and the TRANSEAVER systems [2]. The TRANSEAVER system was developed and tested successfully under the research agreement between the U.S. Arms Control and Disarmament Agency and Japan Atomic Energy Research Institute. Almost all functions which had been demonstrated by the TRANSEAVER and the RECOVER systems are realized on this system, such as timely detection capability, unattended mode operation, secure and reliable communication, and low operation cost performance. In addition, the performance and security of the communication are improved by introducing a new algorithm to handle a set of random numbers which are used as the keys for data enciphering.

Taking the rapid progress in computer hardware into account, the size and weight of a system is not directly concerned with actual use of such a system in near future, but transportability of the software system is. Therefore, the system control programs have been written by the C-language except some I/O handler routines. The hardware of this system is composed of commercially available equipments and units as well as possible regardless of their size and weight.

The system is divided into two subsystems, one is the Grand Command Center (GCC) system and the other is the facility subsystem including containment and surveillance (C/S) sensors. The GCC system consists of two engineering workstations with graphic terminals and two communication control equipments (CCE). The facility subsystem consists of On-site Multiplexer (OSM), Monitoring Unit (MU), Data Terminal Equipment (DTE), Multiplexer Unit (MXU) and C/S sensor including sensor simulator. The communication between two subsystems is controlled by means of a tamper resistant and secure way through the international public telephone line network as shown in Fig. 1. The system configuration is shown in Fig. 2.

2. System Design Concept

The CASDAC system is a physical security and authenticated communication system which continually monitors any changes in the status of C/S sensors and the status of integrity and health of the system itself in order to satisfy the function to monitor remotely containment and surveillance measures sufficiently.

Communication data must be secure and reliable, therefore all the data on public telephone line network are encrypted to prevent falsification and tapping by unauthorized persons, and the high level data link control (HDLC) procedures are adopted to detect tampering with the data or unauthorized polling trial through public telephone line.

The system is designed to realize requirements of secure communication, tamper resistant and tamper indicating functions, very low false alarm rates, and unattended operation of facility subsystems. Together with these requirements, cost performance, easy maintenance, and transportability of the system control programs are also important factors which should be considered.

The basis of the system design is to provide all of the functions demonstrated by the RECOVER and the TRANSEAVER systems and to eliminate some situations pointed out on the feasibility study of the Artemis [3], which have been mainly connected with the performance of data communication.

Since hardware dependent languages had been used for generating system control programs of the TRANSEAVER and also the RECOVER systems, it was so difficult to convert programs on a hardware system to the other advanced one. Moreover, taking into account of rapid progress in computer architecture, a hardware system to be used will be naturally composed of the newest equipments available to use advanced functions depending directly on hardware specifications; such as physical size and weight, response time interval, reliability and etc.. Therefore, it is so important to realize transportability of the system control programs.

In order to embody these requirements as well as practical ones, the UNIX and the MS-DOS operating systems are used for workstation with 32-bit CPU and 16-bit computer respectively, and almost all the system control programs of the CASDAC system have been written by the C-Language in order to make it possible to transfer them easily to a new improved hardware system which will be used actually as secure and reliable remote monitoring system in near future.

3. Grand Command Center (GCC) System

The GCC system consists of a system control and verification unit (CVU) with graphic terminals which is made up of two engineering workstations with 32-bit CPU (68030), and two communication control equipments (CCE). The CCE consists of a 16-bit personal computer (PC9801Vm11), a HDLC control board (PC-COM/V50E,E2) and a modem (DATAX SP2424).

The CVU is the key station of the CASDAC system to be able to control and monitor up to 80 OSMs and all the data monitored are stored in a database and analyzed to detect and distinguish an anomaly status. When the anomaly is detected, the CVU reports automatically it to the proper bodies which must follow up the anomaly status concerned.

The principal function of the CCE is to control telecommunication with a facility subsystem and to carry out encryption of data to be transmitted and decryption of received data.

The UNIX operating system is used for workstations of the CVU and the graphic terminals. The UNIFY, a database management program, is applied to build up a specially designed database to manage all the data monitored by the system, so as to store the collected data and to make check and review (verification) of them systematically. The X-Window system is facilitated to make man-machine interface easy and to display information on the graphic terminal. The C-Language is used for all of the programs including interface programs to link them to the UNIFY and the X-Window.

The MS-DOS operating system is used for a 16-bit personal computer of the CCE. The programs to control the CCE is written by the C-Language.

Finally the GCC system has made available of the following functions;

1) re-initialization of a facility subsystem (OSM, MUs and MXU),
2) response to the urgent call from a facility subsystem due to detecting a alert signal at the OSM, requirement of message transfer from the DTE or requirement of data transfer from the MXU,
3) automatic polling of a facility subsystem to monitor its current status,
4) manual polling of a facility subsystem to monitor its current status,
5) polling of a facility subsystem to send a message to the DTE or a set of data to the MXU,
6) filing the status and C/S data information on the database,
7) analyzing the received status information and arising anomaly signals if the result is distinguished as an abnormal state,

8) filing the anomaly data with associated information into the database,
9) sending automatically this anomaly information to the facsimiles of the proper bodies which must follow up the status concerned,
10) resisting the record about an unauthorized polling trial to the system (GCC, OSM or MU), but no response to that polling.

4. Facility Subsystem

The facility subsystem consists of: 1) The On-Site Multiplexer (OSM) composed of a personal computer, a modem, two HDLC control boards, and a monitoring unit adapter (MU-ADP) which is designed for this system specially to make available of the communication between the OSM and MUs (up to 30 MUs), 2) A set of the Monitoring Units (MU), which can collect up to 8 bits binary (on/off) signals from C/S sensor, 3) The Data Terminal Equipment (DTE) for making available of message transmission between the GCC and the facility subsystem by a classified and secure way, which also consists of a personal computer with 40 M bytes harddisk and a HDLC control board, and 4) The Multiplexer Unit (MXU) which can link with computer controlled devices such as the global positioning system and the satellite communication control equipments of the TRANSEAVER system, but is not included in this system now.

4.1 On-site Multiplexer (OSM)

The OSM is the highest level computer based device to control all other devices within a facility subsystem according to preset instructions stored internally or remote instructions from the GCC.

The principal functions of the OSM are collection of data from MUs, and the MXU, transmission of these data and state-of-health data to the GCC, and message transfer between the GCC and the DTE. A data transmission to the GCC is initiated by either the request from the GCC or the automatic polling from the OSM to the GCC which is triggered by an alert signal aroused within the OSM by monitoring the status signals.

The MU data is collected at programmable time intervals with a random variation of the order of polling sequence through a party line network. One OSM can monitor up to 30 MUs by three party lines (10 MUs for each party line).

The OSM initiates a poll of the MU by sending a request of initialization consisting of 7 bytes followed by an encryption key. The request identifies the MU, and the cipher key and the random number are used together at the MU for enciphering of the response data from the MU. While

8) filing the anomaly data with associated information into the database,
9) sending automatically this anomaly information to the facsimiles of the proper bodies which must follow up the status concerned,
10) resisting the record about an unauthorized polling trial to the system (GCC, OSM or MU), but no response to that polling.

4. Facility Subsystem

The facility subsystem consists of: 1) The On-Site Multiplexer (OSM) composed of a personal computer, a modem, two HDLC control boards, and a monitoring unit adapter (MU-ADP) which is designed for this system specially to make available of the communication between the OSM and MUs (up to 30 MUs), 2) A set of the Monitoring Units (MU), which can collect up to 8 bits binary (on/off) signals from C/S sensor, 3) The Data Terminal Equipment (DTE) for making available of message transmission between the GCC and the facility subsystem by a classified and secure way, which also consists of a personal computer with 40 M bytes harddisk and a HDLC control board, and 4) The Multiplexer Unit (MXU) which can link with computer controlled devices such as the global positioning system and the satellite communication control equipments of the TRANSEAVER system, but is not included in this system now.

4.1 On-site Multiplexer (OSM)

The OSM is the highest level computer based device to control all other devices within a facility subsystem according to preset instructions stored internally or remote instructions from the GCC.

The principal functions of the OSM are collection of data from MUs, and the MXU, transmission of these data and state-of-health data to the GCC, and message transfer between the GCC and the DTE. A data transmission to the GCC is initiated by either the request from the GCC or the automatic polling from the OSM to the GCC which is triggered by an alert signal aroused within the OSM by monitoring the status signals.

The MU data is collected at programmable time intervals with a random variation of the order of polling sequence through a party line network. One OSM can monitor up to 30 MUs by three party lines (10 MUs for each party line).

The OSM initiates a poll of the MU by sending a request of initialization consisting of 7 bytes followed by an encryption key. The request identifies the MU, and the cipher key and the random number are used together at the MU for enciphering of the response data from the MU. While

the encryption key stored in the MU will not be changed until the next re-initialization is instructed by the OSM, the random number is, however, changed by the OSM for every poll.

The response data from the MU consists of the identification of itself, state-of-health information, and the present and past history of sensor status information. In addition, the number of responses counted by polling counter of the MU is contained, which is used to detect any unauthorized poll of the MU. If this number is different from the number recorded in the OSM, it is an evidence that a third party has performed unauthorized polling or the MU signaling and that an attempt has been made to breach the security of the system, such a polling counter mismatch is a condition for generating a system alert. The same function is also facilitated in the communication protocol between the OSM and the GCC.

The OSM is the most important node for unattended operation of the facility subsystem, so that security of the OSM must be maintained in the highest level. The OSM, therefore, is protected by a secure cover and is capable of enciphering all the communication data between the OSM and the CCE. The OSM is naturally equipped with self-check capabilities and it reports its state-of-health to the GCC.

4.2 Monitoring Unit (MU)

The purpose of the MU is to monitor continuously sensor status up to 8 bits and to transmit them to the OSM. The MU is built around a 8-bit micro-processor with 128 bytes memory (RAM), and it has a self-check capability and provides of state-of-health reports to the OSM. The current status and history data stored temporary in the memory are automatically transmitted to the OSM. In addition, the MU also encrypts the data which are sent to the OSM, because the communication line between the MU and the OSM lies typically in an unprotected cable.

The MU has a 16-byte key for encryption which can be replaced with a new one by re-initialization carried out by the GCC through the OSM. The MU is designed to be compact, 8 x 20 x 6 (cm) in dimension, and it is connected with its associated sensors.

4.3 Data Terminal Equipment (DTE)

The DTE is a 16-bit personal computer with a 40 M bytes hard disk and is used as a terminal to make available of message data communication between the GCC and a facility subsystem through the OSM. The message must be in an ASCII file and the file length is limited up to 8 k bytes, which can be

provided on an editor or word-processor such as WORDSTAR to be available on the DTE.

This message data communication will be required by the authorized person to transmit a urgent message from the DTE to the GCC or vise versa.

For data security concerns, the access to the DTE is limited by means of passwords. The received message is stored on the hard disk with its own file name that has a number changing cyclically up to 64 (64 files), and the contents can be reviewed and checked on the display monitor.

5. Structure of Communication Data

The data communication between the OSM and the GCC is controlled by the High level Data Link Control (HDLC) procedure, on which the communication is curried out by transmitting a framed message data with definite fields for the HDLC protocol.

One packet of the data consists of one byte preamble, one byte polling address field, one byte control command field, an information field, two bytes frame check sequence data field for cyclic redundancy check (CRC), and one byte postamble.

The polling address and control command fields are for the HDLC protocol, and the received data is checked by the CRC within the packet.

The information field consists of either no field or a header field with 8 bytes length only or the header field followed by a 128 bytes of data field (total 136 bytes). The header is used to assign the attribute of the information field and to control a specific communication procedure that has been developed for the CASDAC system.

5.1 Header Field

The header field consists of the following six parameters labeled by DID, CID, VDL, KEY, RNO and STS, of which definitions and word length are given as follows:

1. DID (1 byte) : Data Identification (Command or Response)
2. CID (1 byte) : Continuity of Information Data
3. VDL (2 bytes) : Valid Data Length
4. KEY (1 byte) : Tag of Key Number
5. RNO (1 byte) : Tag of Random Number

provided on an editor or word-processor such as WORDSTAR to be available on the DTE.

This message data communication will be required by the authorized person to transmit a urgent message from the DTE to the GCC or vise versa.

For data security concerns, the access to the DTE is limited by means of passwords. The received message is stored on the hard disk with its own file name that has a number changing cyclically up to 64 (64 files), and the contents can be reviewed and checked on the display monitor.

5. Structure of Communication Data

The data communication between the OSM and the GCC is controlled by the High level Data Link Control (HDLC) procedure, on which the communication is curried out by transmitting a framed message data with definite fields for the HDLC protocol.

One packet of the data consists of one byte preamble, one byte polling address field, one byte control command field, an information field, two bytes frame check sequence data field for cyclic redundancy check (CRC), and one byte postamble.

The polling address and control command fields are for the HDLC protocol, and the received data is checked by the CRC within the packet.

The information field consists of either no field or a header field with 8 bytes length only or the header field followed by a 128 bytes of data field (total 136 bytes). The header is used to assign the attribute of the information field and to control a specific communication procedure that has been developed for the CASDAC system.

5.1 Header Field

The header field consists of the following six parameters labeled by DID, CID, VDL, KEY, RNO and STS, of which definitions and word length are given as follows:

1. DID (1 byte) : Data Identification (Command or Response)
2. CID (1 byte) : Continuity of Information Data
3. VDL (2 bytes) : Valid Data Length
4. KEY (1 byte) : Tag of Key Number
5. RNO (1 byte) : Tag of Random Number

6. STS (2 bytes) : Status of Data Communication

(1) DID : Data Identification
The DID is used for the CASDAC communication protocol such as the command message from the GCC to the OSM or the responses message corresponding with the command.

(2) CID : Continuity of Information Data
CID = 1; The first packet of the information data
CID = 2; The last packet of the information data
CID = 3; A single independent packet
CID = 0; Intermediate packet

(3) VDL : Valid Data Length
The valid data length defines the length of valid data in the data field.

(4) KEY : Tag of Key Number
This is the tag identification for the cipher key table which consists of 256 random numbers. The length of each random number in the table is 128 bytes.

(5) RNO : Tag of Random Number
This is the tag identification for the random number which is the same as the cipher key table.

(6) STS : Status of Data Communication
The STS is used for identifying the current status of data communication including error status, or for notifying to the GCC that there are some data in DTE or MXU to be transmitted.

5.2 Data Field

The data field has 128 bytes fixed length, and is reserved for message data to be transmitted, all of which are naturally enciphered by a cipher key and a random number.

A typical format of this data field is to be seen in the data about the current status of facility subsystem and C/S sensors to be sent back to the GCC. The format is defined uniquely by DID in the header and interpreted correctly.

6. Status Data

The GCC collects and analyzes status data from the OSM through the public telephone line network in order to monitor the status of C/S measures including the integrity and health of the monitoring system itself. The following is the definitions of status data collected by the CASDAC system.

6.1 OSM Status(1)

bit	Definition
0)	No key data in the OSM
1)	"AC" power recovered
2)	Battery power recovered
3)	reserved
4)	reserved
5)	reserved
6)	reserved
7)	reserved

The change in each status bit from "OFF" to "ON" is resulted by the following reason or course respectively:

1) No MU Key in OSM; bit 0 = "ON",
No key data for MUs in the OSM which is used for encryption of communication data between the OSM and MUs. MUs must be re-initialized from the GCC in order to recover them.

2) "AC" power recovered; bit 1 = "ON",
The AC power had been cut out for shorter periods than 72 hours (3 days) but now it is supplied to. The OSM recovers automatically, and reports it to the GCC.

3) Battery power recovered; bit 2 = "ON",
The AC power of the OSM had been cut out for longer periods than 72 hours. All of the system control programs and data in the OSM had been erased. Therefore they must be re-installed into the memory from the floppy disk at facility site.

Notes: Tampered (no bit assign)
The exterior container (box) of the OSM had been opened.
All of the system control programs anddata in the OSM were erased. Therefore they must be re-installed by reading them into the memory from the floppy disk at a facility site.

6.2 OSM Status(2)

bit	Definition
0)	Unauthorized call
1)	Data format error
2)	Communication error
3)	reserved
4)	reserved
5)	reserved
6)	reserved
7)	reserved

The change in each status bit from "OFF" to "ON" is resulted by the following reason or course respectively:

1) Unauthorized call; bit 0 = "ON",
The OSM received a call for requesting to link with, but the address in the received packet is not consistent with the authorized one.

2) Data format error; bit 1 = "ON",
At least, one of the following error is observed in the data received by the OSM.

i) Error in the function and format of the data received,
ii) Error in the communication protocol sequence,
iii) Mismatch in the data length compared with the declared one.

3) Communication error; bit 2 = "ON",
The CRC algorithm detects errors in a data packet or the time-out algorithm detects the unacceptable time delay for receiving a response data.

6.3 MU Status

bit	Definition
0)	Cutting sensor signal cable off
1)	External power recovered
2)	reserved
3)	reserved
4)	Message format error
5)	reserved
6)	reserved
7)	reserved

The "ON" status of the bits 0, 1 and 4 are resulted by the followings respectively:

1) Cutting sensor signal cable off; bit 0 = "ON",
   The cable which is linked between a C/S sensor and a MU was cut off.

2) External power recovered; bit 1 = "ON",
   The DC power supplied from the OSM had been cut out, but now it is recovered.

3) Data format error; bit 4 = "ON",
   Error either in the format of the data received from the OSM or in the sequence in the communication protocol.

6.4 Inferred MU Status

bit	Definition
0)	No MU response
1)	Error in MU response function
2)	Error in communication with MU
3)	MU polling counts mismatch
4)	Inconsistent past historical data
5)	reserved
6)	reserved
7)	No key data in MU

The status bits of 0 to 4 and 7 are set to "ON" when the OSM infers the followings are happened in the MU respectively:

1) No MU response; bit 0 = "ON",
   No response from the MU is confirmed for the three consecutive requests for asking the MU status.

2) Error in MU response function; bit 1 = "ON",
   The response function from the MU does not correspond with the command function that was sent out to the MU.

3) Error in communication with MU; bit 2 = "ON",
   At least, one of the followings is detected in the data received from the MU.

   i) Parity Error
   ii) Framing Error
   iii) BCC Error (BCC; Block Check Character)

iv) Inconsistent MU address
v) Time-over for response time of MU

4) MU polling counts mismatch; bit 3 = "ON",
The number in the polling counter register of the OSM is not consistent with that of the MU.
After bit 3 is set to "ON", the number in the OSM polling counter is set to the same number in the MU polling counter, then the OSM continues the polling procedure to call the MU.

5) Inconsistent past historical data; bit 4 = "ON",
The past historical data received just now from the MU is not consistent with the data that had been received as the current status data previously.

6) No key data in MU; bit 7 = "ON",
The MU sends back the data that there is no key data for enciphering in the MU, then the communication with the MU is terminated.

NOTES: All informations in this inferred MU status are set in the OSM.

6.5 C/S Sensor Status

bit	Definition
0)	C/S sensor bit-#1
1)	C/S sensor bit-#2
2)	C/S sensor bit-#3
3)	C/S sensor bit-#4
4)	C/S sensor bit-#5
5)	C/S sensor bit-#6
6)	C/S sensor bit-#7
7)	C/S sensor bit-#8

The "ON" state of each C/S sensor signal from bit-#1 to bit-#8 shows the fact that the sensor has detected anomaly status or the cable line to connect with the sensor has been cut off.

7. Security Measures

It is essential to be secure and reliable against any wire tapping and unauthorized intervention concerning the data communication between the OSM and the GCC through the public telephone line network.

The CASDAC system provides the following counter measures against unauthorized intervention and wire tapping.

LEVEL-1 Automatic Communication Channel Release by HDLC

Based on the adoption of the HDLC protocol, the communication control procedure makes available of the function that is capable of consistency checks about the frame structure and the protocol procedures such as length, format, sequence number, the order of command and response and the address of the port, etc..

The communication channel is automatically released whenever, at least, an inconsistent one or error is detected by the HDLC protocol.

LEVEL-2 Automatic Termination of Data Communication

A special communication control protocol has been implemented into the CASDAC system on application program level. This protocol also discriminates errors in the communication procedures, the format of the header, the length of the data field and the order of command and response specified in the header field.

The communication between the GCC and the OSM is terminated due to any error detected on this level.

LEVEL-3 Discrimination of Unauthorized intervention

Using the function of the polling counts mismatch test, the GCC can easily recognize and distinguish the fact that some trials to make trespass on the OSM had been made through the public telephone line network.

Any call accepted by the OSM is counted on the polling counter registers facilitated in the GCC and the OSM. This number recorded by the OSM is sent back to the GCC and compared with that in the GCC.

Moreover, a secret number with 4 byte word length is written by the GCC in the very beginning of the data field with a specific command, and the number is sent back from the OSM as a response at the next polling. The GCC checks consistency of these two numbers in order to confirm that no intervention had been done since the last polling.

These functions make it available to detect any unauthorized intervention or access to either the OSM or the GCC through the international public telephone line network.

LEVEL-4 Encryption of Data in The Data Field

The algorithm used for data enciphering is identical with that used in the RECOVER and the TRANSEAVER systems.

All data including message in the data field are enciphered. Two independent random numbers (Key Data and Random Number) are used for the cipher and selected randomly from the file for each data transmission, in which 256 tagged random numbers with 128-byte words length are filed. This file is stored in the main memory both the OSM and the CCE at the time when the system control program is installed into them respectively.

There are quite large number of combinations in the selection, and the combination is changed every data transmission. Moreover, unauthorized persons never have a chance to access to the set of random numbers through the public telephone line network. Therefore, the enciphered message data is secure and confident enough to protect it against any wire tapping or unauthorized intervention.

8. Other Measures for Security

8.1 Re-initialization of Facility Subsystem

In any of abnormal states of the system program where at least one of the parameters in the RAM or registers is lost or inconsistent, the OSM and its associated MUs must be re-initialized in order to return to its normal state.

The re-initialization can be done remotely by a demand call of the GCC, and is one of the most important features of the CASDAC system. It involves the following functions:

1) reset all variables and clear status information stored in the OSM,
2) replace the CCE telephone number in the OSM if necessary, and
3) replace the cipher key data stored in the MUs with new ones.

These functions have been adopted to meet the requirements concerning the security of data stored in the OSM and the capability of unattended operation of the facility subsystem.

These functions make it available to detect any unauthorized intervention or access to either the OSM or the GCC through the international public telephone line network.

LEVEL-4 Encryption of Data in The Data Field

The algorithm used for data enciphering is identical with that used in the RECOVER and the TRANSEAVER systems.

All data including message in the data field are enciphered. Two independent random numbers (Key Data and Random Number) are used for the cipher and selected randomly from the file for each data transmission, in which 256 tagged random numbers with 128-byte words length are filed. This file is stored in the main memory both the OSM and the CCE at the time when the system control program is installed into them respectively.

There are quite large number of combinations in the selection, and the combination is changed every data transmission. Moreover, unauthorized persons never have a chance to access to the set of random numbers through the public telephone line network. Therefore, the enciphered message data is secure and confident enough to protect it against any wire tapping or unauthorized intervention.

8. Other Measures for Security

8.1 Re-initialization of Facility Subsystem

In any of abnormal states of the system program where at least one of the parameters in the RAM or registers is lost or inconsistent, the OSM and its associated MUs must be re-initialized in order to return to its normal state.

The re-initialization can be done remotely by a demand call of the GCC, and is one of the most important features of the CASDAC system. It involves the following functions:

1) reset all variables and clear status information stored in the OSM,
2) replace the CCE telephone number in the OSM if necessary, and
3) replace the cipher key data stored in the MUs with new ones.

These functions have been adopted to meet the requirements concerning the security of data stored in the OSM and the capability of unattended operation of the facility subsystem.

8.2 Confidence of Data

All data in a frame to be transferred between an OSM and the GCC are encoded by CRC function for bit error detection within HDLC protocol. If any bit error is detected in a frame, the protocol retries automatically to transmit the frame up to three times. In order to assure the confidence further, all data received from the OSM or the GCC are monitored about the consistency of the information in the header field especially Data Identification (CID), Continuity of Information Data (DID) and Valid Data Length (VDL). If an inconsistency is detected, the frame is discarded.

8.3 Security of Data in Memory

Data encryption and tamper indication are the primary techniques for maintaining security of the system. In addition, the OSM is designed so that all information stored in memory are erased by opening its cover.

9. Reliable Operation

When power failure occurs in an OSM, a back-up power system maintains all data in the OSM memory and the OSM continues to poll all MUs for one hour after power down. If the primary power is lost for more than one hour, the polling of the MUs is suspended and the OSM goes into "asleep mode" for up to 72 hours (3 days). If the primary power is activated within 72 hours, the OSM resumes normal operation.

However, after 72 hours in the "asleep mode", all data in the memory of the OSM are lost and the OSM never return automatically to the normal operation mode unless the initialization procedures are taken at the facility site.

8.2 Confidence of Data

All data in a frame to be transferred between an OSM and the GCC are encoded by CRC function for bit error detection within HDLC protocol. If any bit error is detected in a frame, the protocol retries automatically to transmit the frame up to three times. In order to assure the confidence further, all data received from the OSM or the GCC are monitored about the consistency of the information in the header field especially Data Identification (CID), Continuity of Information Data (DID) and Valid Data Length (VDL). If an inconsistency is detected, the frame is discarded.

8.3 Security of Data in Memory

Data encryption and tamper indication are the primary techniques for maintaining security of the system. In addition, the OSM is designed so that all information stored in memory are erased by opening its cover.

9. Reliable Operation

When power failure occurs in an OSM, a back-up power system maintains all data in the OSM memory and the OSM continues to poll all MUs for one hour after power down. If the primary power is lost for more than one hour, the polling of the MUs is suspended and the OSM goes into "asleep mode" for up to 72 hours (3 days). If the primary power is activated within 72 hours, the OSM resumes normal operation.

However, after 72 hours in the "asleep mode", all data in the memory of the OSM are lost and the OSM never return automatically to the normal operation mode unless the initialization procedures are taken at the facility site.

10. Tests and Evaluations

The tests of the CASDAC system are categorized into two phases, one is the function test to check and confirm the functional performance of the system, the other is the communication test to demonstrate its reliability for long period of time.

10.1 Function Tests

For the function tests, the GCC and two facility subsystems were set up in JAERI/Tokai. The GCC was, of course, linked to these facility subsystems through the public telephone line network. Then, the basic functions regarding tamper resistance and indication and response of anomaly detection were tested in our laboratory.

It is so difficult to protect or guard a facility subsystem by means of hardware structures against tampering attempts, so that almost all the functions are attained by system control programs implemented, except the cover case of an OSM.

1) Cable Line Intrusion Test

There are cable lines connecting OSM with MUs, DTE and MXU within a facility subsystem as shown in Fig.s 1 and 2. The cable lines connecting between an OSM and MUs can not be protected usually by intrusion sensors or surveillance system but the others. Therefore, cable line intrusion tests have been conducted by focusing on the lines connecting between an OSM and MUs, and between a MU and a sensor.

a) If a communication line between the OSM and a MU is broken, the OSM detects it at a polling of the MU via the line, then initiates calling to the GCC to report anomaly condition of "no MU response".

b) If a sensor signal line between a MU and a sensor is broken, the OSM detects it, then initiates calling to the GCC to report anomaly condition of "Cutting sensor signal cable off and anomaly of sensor".

c) If a power line between an OSM and a MU is broken, the MU enters "asleep mode" to keep sensor status monitored. The OSM detects no response from the MU, then initiates calling to the GCC to report anomaly condition of "no MU response".

When the power is recovered, the OSM initiates calling to the GCC to report "External Power Recovered".

d) If AC power line for an OSM is broken, the OSM enters "asleep mode" to keep monitored status but no communication with the GCC. The GCC could detect no response from the OSM or communication error. When the power is recovered within 72 hours, the OSM recovers automatically its operation, then initiates calling to the GCC to report "AC Power Recovered".

e) If the telecommunication line is broken, there is no way to test it directly, but the GCC could detect such a break as communication impossible or communication error.

2) Statistics of Anomaly Detection Time

There are three levels of hierarchy to detect and save anomalies in the CASDAC system. The first level is in a MU to detect and save the status changes of sensors, the second is in an OSM to detect and save the status of state-of health of the OSM and to monitor the status stored in MUs, the last is in the GCC. All status changes detected by MUs or OSMs are saved temporally and transmitted to the GCC through the international public telephone line network. The GCC analyzes them to detect and distinguish anomaly status and reports the status to right bodies that must take a follow up action about the anomaly situation.

a) Time lag in a MU

A MU monitors sensor status every one second and the status bits in the MU are updated when a unique status is observed consecutively four times. Therefore, the time lag to detect status changes of sensor is about 5 seconds.

b) Time required in the data transfer from a MU to an OSM

The time required to transfer one byte data between an OSM and a MU is about 37 m sec. Therefore, the time required to complete a communication is follows:

Initialization of MU : 8 sec/MU
Normal polling : 15 sec/MU

However, the polling rate of one MU depends on the number of MUs connected with the OSM and the order of the pollings which is assigned randomly by the OSM within a series of MU pollings.

c) Time lag in an OSM

There is no large time lag in an OSM, but there are few seconds for testing the condition for urgent calling to the GCC and data encryption.

d) Time required in the data transfer from an OSM to the GCC
An OSM initiates urgent calling to the GCC, so that there is no idle time for waiting a polling from the GCC. The time required consists of the time lag for linking the telephone line network between the OSM and the GCC and the time required to transfer the status data monitored by the OSM including MU and sensor status. The time required for data transfer is measured by the time while the modem is active and is about 54 seconds in average.

The overall time interval required to complete data transfer, since one bit of a sensor simulator was changed, is also measured in a case that only one MU is connected to the OSM and does not include delay due to a waiting time for retry call when the line is busy . This time is in the range from 64 to 78 seconds and is 74 seconds in average, although this depends on the telephone line network condition.

10.2 Reliability Test

For the reliability tests, the GCC and two facility subsystems were situated in JAERI/Tokai and one was in NEC Tokyo. The GCC was, of course, linked to these facility subsystems through the public telephone line network. The reliability and stability of the communication control system were tested successfully for about two months. Then the test was continued for four months after released the facility subsystem in NEC Tokyo. In this test, two facility subsystems were polled from the GCC frequently and also called the GCC by means of urgent calling triggered by a status change in a MU artificially.

During the communication tests, more than several thousands of polling and few hundreds of urgent callings were curried out, and the communication error statistics is as follows:

HDLC Open error	:	0.2%
Line Busy	:	0.6%
Time Out	:	0.2%

These error records are stored in the database with associated data to trace back what happened at the time. No system error was observed in the records. The system had made recalling automatically just after detection of the error and the communication was performed and completed successfully for all cases.

11. Concluding Remarks

The CASDAC system as an Upgraded RECOVER system has been developed and tested successfully. The hardware of this system is not designed to apply for the Agency safeguards directly, but the software system written by C-language is.

The most functions regarding tamper indication and security of the facility subsystem are realized by the system control program including cipher and communication protocol. The system may be secure and confident enough to meet requirements of the Agency safeguards except the limitation about environ-mental condition to be able to use the OSM and its size and weight, because the OSM is composed of a commercially available personal computer at when the system was designed.

However, taking into account of rapid progress in computer hardware, it seems not to be so difficult to develop a improved hardware of the OSM in use of a new portable computer such as book size computer.

References:

[1]: RECOVER System : REmote COntinual VERification System
This system was developed by US ACDA and tested by IAEA for the use of international safeguards.

F.J. Prokoski,
"Global Monitoring of International Nuclear Safeguards",
Proceedings of the fifth International Conference on Computer Communication, Atlanta, October, 27-30, 1980.

[2]: TRANSEAVER System: TRANsportation by SEA VERification System
This system was developed and tested successfully under the research agreement between the US Arms Control and Disarmament Agency (US ACDA) and Japan Atomic Energy Research Institute (JAERI).

N. Kyriakopoulos, H. Kuroi and O.J. Sheaks,
"TRANSEAVER: A Security System for International Sea Transport",
IEEE International Conference on Communications '86,
Toronto, Canada, June, 22-25, 1986.

[3]: Artemis System : Aircraft Real Time Encrypted Monitoring and Information System
Feasibility study was done by The MITRE Corporation sponsored by US ACDA and JAERI.

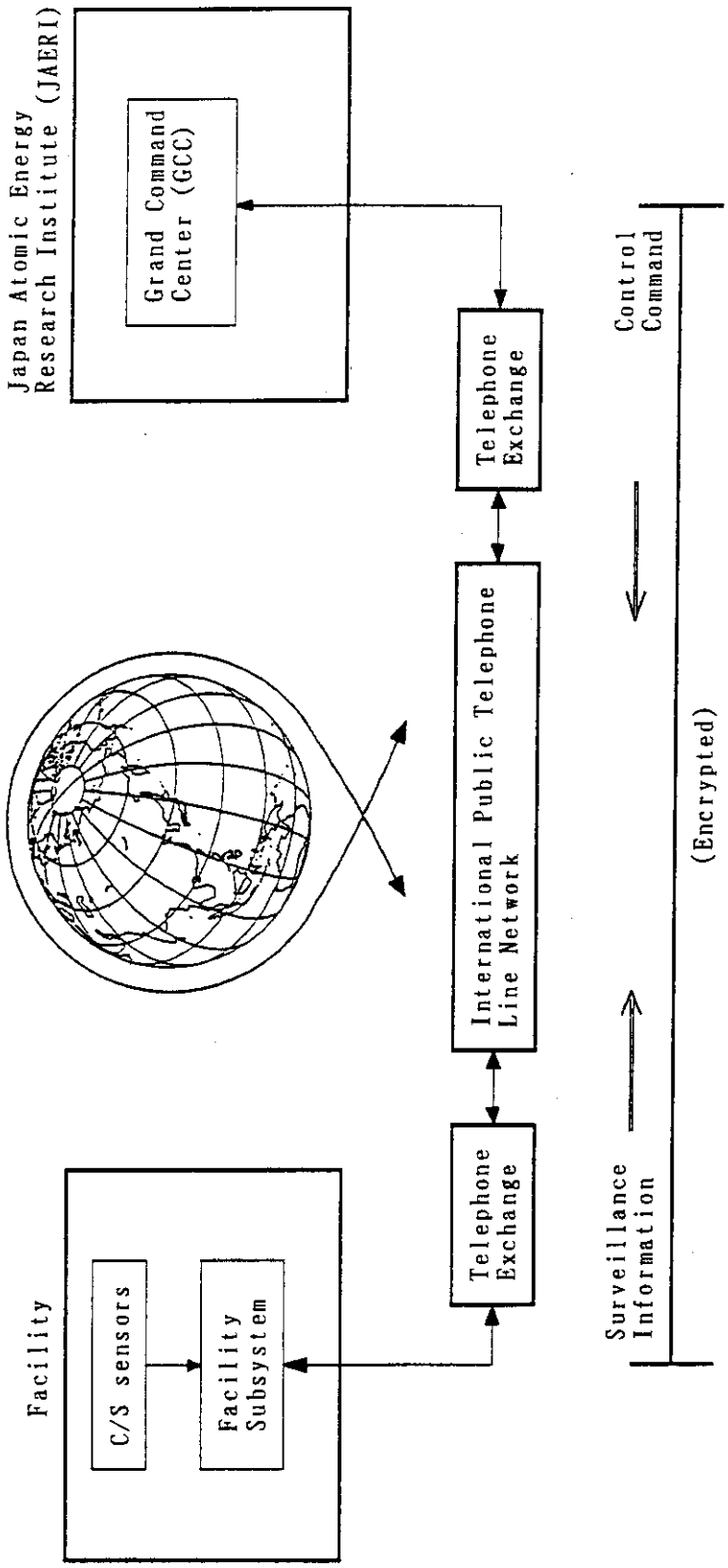

Fig. 1 Concept of CASDAC System

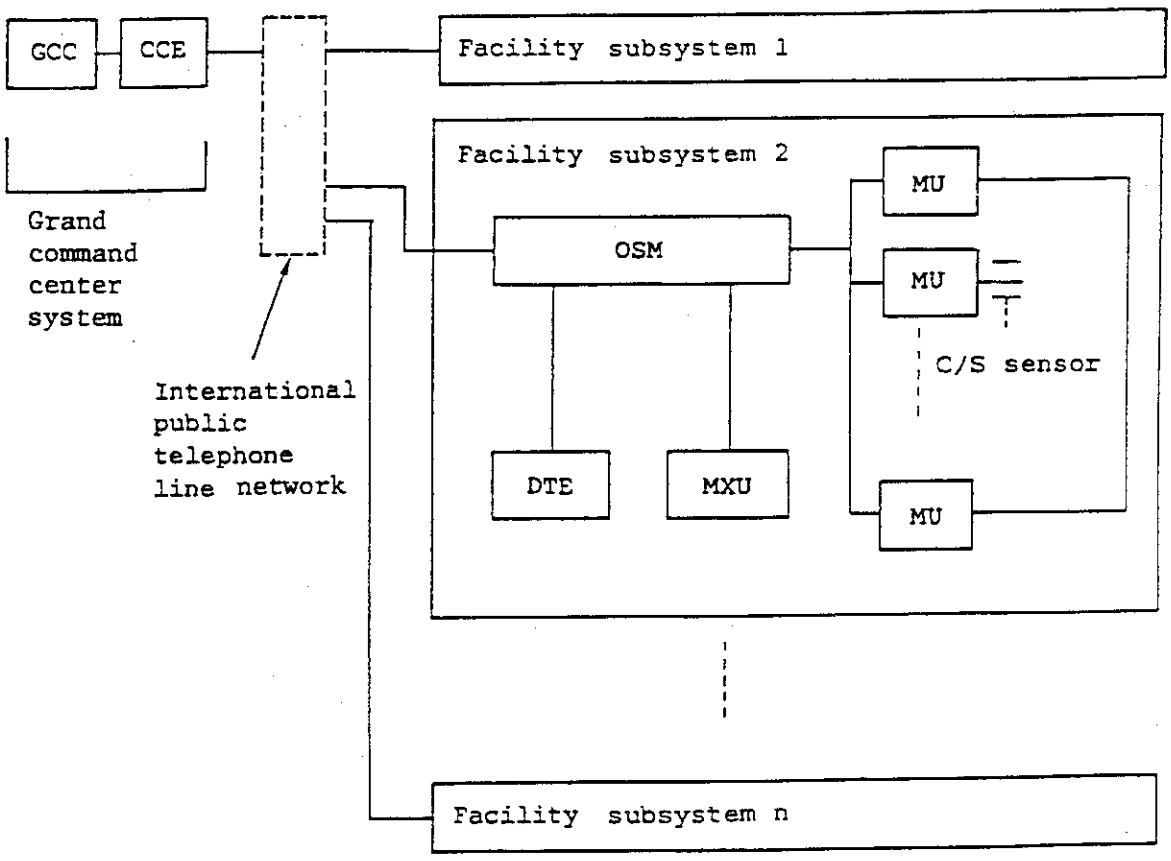

Fig. 2 Configuration of CASDAC System