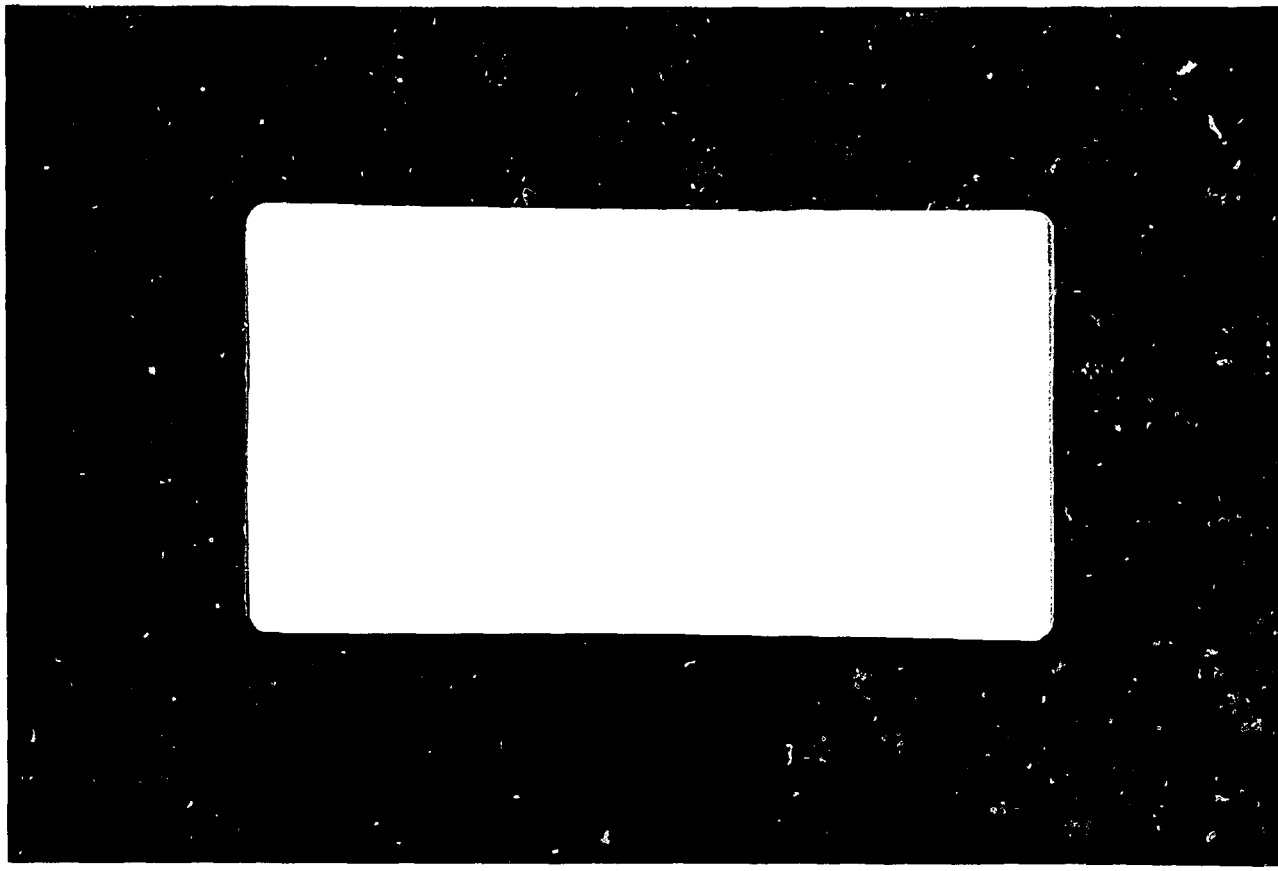


Work Performed Under Contract DE-AC09-78ET01040

ALLIED-GENERAL NUCLEAR SERVICES
P.O. BOX 847
BARNWELL, SC 29812

AGNS-1040-CONF-67

Distribution
Category UC-83 Special

THE DEVELOPMENT OF AN ADVANCED SAFEGUARDS SYSTEM AS A PROLIFERATION DETERRENT

Arnold A. Ayers
Lawrence D. Barnes

November 1978

Presentation for ANS Winter Meeting
November 12 - 17, 1978
Sheraton Park Hotel, Washington, D. C.

ALLIED-GENERAL NUCLEAR SERVICES
POST OFFICE BOX 847
BARNWELL, SOUTH CAROLINA 29812

PREPARED FOR THE
DEPARTMENT OF ENERGY
FUEL CYCLE PROJECT OFFICE
UNDER CONTRACT DE-AC09-78ET01040

Presentation for ANS Winter Meeting
November 12-17, 1978
Sheraton Park Hotel, Washington, D.C.
By: A. L. Ayers and L. D. Barnes

THE DEVELOPMENT OF AN ADVANCED SAFEGUARDS SYSTEM AS A PROLIFERATION DETERRENT

Potential proliferation of nuclear weapons is of increasing world-wide concern. The United States Government has been particularly outspoken in its concern, and it has expressed policies and taken actions which it presupposes to be positive deterrents to proliferation. These actions have included, among other things, the termination of licensing proceedings related to the recycle of mixed oxide fuel in the United States and the formation of the International Nuclear Fuel Cycle Evaluation to study alternative proliferation resistant fuel cycles for light water and other nuclear power reactors. Nuclear energy critics now include proliferation, along with safety and waste, as a reason, or at least rationale, for their opposition to nuclear power. Proliferation is thus primarily a matter of political and institutional concern. Such concern is, to a large extent, independent of technology; key elements in nuclear technology have been widely disseminated throughout the world in unclassified publications.

Near term technology does not provide the means for altering plutonium so that its use in a nuclear explosive device is incredible.

We do have the capability to develop means to make diversion or theft of plutonium or other Strategic Special Nuclear Material (SSNM) extremely improbable. If SSNM is effectively controlled, then, either a systematic diversion or a one-shot theft becomes an unlikely scenario for proliferation. Thus, reprocessing becomes a relatively likely route to proliferation. This rationale was used in developing the safeguards program which Allied-General Nuclear Services (AGNS) is conducting for the U. S. Department of Energy. The development of an Advanced Safeguards System to provide a truly effective level of control for SSNM at a nuclear fuel reprocessing plant has been established as the objective of this program which AGNS is carrying out at the Barnwell Nuclear Fuel Plant (BNFP). Such System will, when fully implemented, provide an in-depth defense against theft or diversion of SSNM or of sabotage, either by prevention of the act or by timely detection coupled with appropriate ameliorative counteraction. Defense in depth is obtained by coordinating information from all possible sources such as plant instrumentation, operations, maintenance, radiation protection, physical protection, nuclear material control, etc., on a near real-time basis to defer, defeat, or detect maleficent acts promptly.

A 1500 MTU-per-year Separations Facility has been constructed at Barnwell, South Carolina, for the recovery of uranium and plutonium from spent fuel from nuclear power reactors using the chop-leach adaption of the Purex process. Construction of a facility for conversion of uranyl nitrate to UF_6, using the process which has been successfully employed for many years at Allied Chemical's Metropolis, Illinois Plant, has also been constructed at the Barnwell site. The Separations Facility was in the process of obtaining an

operating license when operation of privately owned commercial nuclear fuel reprocessing plants was indefinitely deferred in the United States by President Carter on April 7, 1977. Since December of 1977, the AGNS technical staff has been conducting a Research and Development (R&D) Program for the Department of Energy which includes evaluation of the installed safeguards system during simulated (i.e, nonradioactive) operation of the BNFP and the development of concepts for an Advanced Safeguards System. In selecting concepts for the Advanced System, the AGNS staff has made extensive use of the excellent R&D efforts that have been carried out at DOE sites such as Sandia Laboratories, Lawrence Livermore Laboratory, Los Alamos Laboratory, Idaho National Engineering Laboratory, Brookhaven National Laboratory, etc.

The Advanced Safeguards System, as presently conceived, consists of three major parts:

(1) Computerized Nuclear Materials Control and Accounting System (CNMCAS)
(2) Physical Protection System (PPS)
(3) Safeguards Coordination Center (SCC).

Each of these parts will be discussed in turn with first a brief description of what the AGNS staff now thinks they will ultimately contain when fully developed, what part is presently installed, the results of testing to date, and plans for future testing.

Computerized Nuclear Materials Control and Accounting System (CNMCAS)

The Computerized Nuclear Materials Control and Accounting System contains a modular network of computers and communications equipment with auxiliary data collection, storage, and retrieval devices. When completed, it will consist of the following:

- Laboratory data subsystem to assemble all data associated with analysis of plant samples and to provide access to these data for other parts of the CNMCAS system. Major analytical instruments will transmit results directly to the computer to minimize errors such as transposition of figures in results.

- A measurement subsystem to collect and generate data for calculating the material balance components of input, product, waste, and inventory. Process instrumentation for measuring liquid-level, density, and temperature of liquids in process vessels is connected to CNMCAS through a real-time peripheral (RTP) data acquisition system.

- A nuclear materials accounting subsystem to provide for real-time accounting of special nuclear material. Nuclear materials accounting as required by regulations and contractual arrangements, as well as fungible and transaction accounting, will be included.

- A measurement control subsystem to establish quality of measurement data as it is generated. Measurement uncertainties from limits of error

calculations will be based on current measurements and will be available on demand. The system will be designed to promptly identify measurements that are out of control so corrective action can be taken.

- An item and seal control subsystem to provide current knowledge of identities, quantities, and location of discrete items containing SNM. Current information regarding each discrete item, seal, and tamper-safing device will be maintained at all times.

- A physical inventory subsystem to determine and verify in-plant (vessels and items) SNM quantities for each Material Balance Area. Ultimately, it is hoped to establish near real-time inventory measurements.

- A process monitoring and surveillance subsystem to monitor dynamic sections of the process, including transfers between process vessels, and to provide surveillance on normally static vessels and sumps.

- A subsystem to interface with the Department of Energy's (DOE) Nuclear Materials Management and Safeguards System (NMMSS), which maintains a data base of nuclear materials transactions within the United States. When the SCC is fully developed, these data will go to NMMSS through the SCC.

- A subsystem to interface the CNMCAS with the SCC. The SCC coordinates operations, physical security, nuclear materials management, and other departmental functions and serves as a communications link between these functions. Requests for authorization, authorization of actions affecting

SNM, and information concerning or affecting SNM status and control will be carried through this interface.

The multiple interfaces between the CNMCAS subsystems are given in Figure 1 which diagrams these interfaces.

The bulk of the hardware for CNMCAS has been installed, and it was used during recent simulated operations using natural uranium as a stand-in for SNM. Software for most of the subsystems is actively being developed. Various parts of these subsystems are being tested more or less sequentially in the plant so that additional steps are being added in manageable increments.

The Laboratory Data Subsystem has been successfully operated for about two years (Figure 2). It consists basically of a PDP 11/35 computer with 64 K of memory, two mag tape transports, two disk drives, and a line printer. Various input/output (I/O) devices are located throughout the laboratories, the plant areas, and in the process control rooms. The LDS is based on the Resource Sharing-Time Sharing (RSTS/E) operating system using the BASIC-PLUS language processor. All incoming samples are logged into the system, and as samples are analyzed, the data are entered and the results are calculated by the system. After the analyst approves a result, this information is available to any terminal on the system. When all constituents for a sample have been completed, a final report is printed on the line printer. Data and results are maintained on disk for 48 hours after final approval and then transferred to magnetic tape for long-term retention (5 years). Two instruments, the mass spectrometer and multichannel analyzer, have been interfaced to the system.

These instruments have their own dedicated minicomputers, and the interface is only for data transfer to the LDS for long-term storage. Other laboratory instruments will be interfaced to the system. These are electronic balances, automatic titrators, densimeters, spectrophotometers, fluorophotometers, coulometers, a gas chromatograph, a leach hulls monitor, and a solid waste monitor.

To accomplish the objectives of the CNMCAS, additional hardware was procured to interface with the LDS (Figure 3). The hardware includes a central processor unit (CPU), and input/output (I/O) devices. Also, real-time peripheral (RTP) data acquisition equipment for the remote monitoring of multiple process parameters from both the Separations and UF_6 facilities and from the Plutonium Nitrate Storage and Load-Out Area is included. The LDS and NMCAS CPU's are connected for interchange of information as required. Also, an automatic switching arrangement may be included. It would allow either CPU to take full control of the CNMCAS if the CPU or any of the memory devices fail on the other system.

Based on experience to date, the installed hardware has the capacity to handle the CNMCAS requirements. However, as the system has developed, its scope has increased, and additional data processing capability and storage capacity may be required. Development work to be continued on each of the subsystems is considered next.

The development of measurement techniques for solution volume density and nuclear material concentration is adequate for current requirements. However,

development and testing of alternate measurement techniques will be continued to improve backup for measurement systems and to meet new requirements. The NDA measurement technique and equipment for the SNM content of hulls require thorough testing. Development of satisfactory NDA equipment for measuring the SNM content in solid waste containers is required.

Software required to interface measurement instrumentation and manipulate measurement data needs additional definition and testing.

Evolving regulations and undefined requirements seriously complicate the design of a complete accounting subsystem. Basic accounting functions can be incorporated in the CNMCAS without major difficulty. However, software design and testing will be a continuing effort.

The elements of a measurement control program for a nuclear fuel reprocessing facility have been satisfactorily detailed. Software for incorporating selected elements in the CNMCAS is being developed for in-plant testing. In addition, measurement innovations will be incorporated in the measurement control subsystem.

A better definition of the mechanics of item and seal control, including item and seal identification hardware, is required, but this design should be quite straightforward when the definition is completed.

Development of physical inventory mechanics is progressing satisfactorily. Software development and testing to complete the design of the physical inventory subsystem is simple but time-consuming.

The design of the physical data link between the CNMCAS and the NMMSS (Nuclear Materials Management and Safeguards System) is not complex. It requires definition of the data to be transmitted and developing and testing the software to accumulate and transmit these data. The completed design of the nuclear materials accounting subsystem is required for the CNMCAS-NMMSS interface subsystem.

Additional hardware (capable of interfacing with CNMCAS) will be selected to complete the design of the process monitoring/process surveillance subsystem such as:

(1) Valve position indicators
(2) Tamper-safing devices
(3) In-line sensors for applicable parameters (i.e., pressure, flow, conductivity, radiation, etc.).

Software development and testing to complete the design of this subsystem can be complex, and it will stretch our ingenuity. Evolving regulations and requirements may impact hardware selection and software design.

Initial definition of the CNMCAS-SCC interface subsystem can proceed, but design of the subsystem must go hand-in-hand with the development of the SCC.

The security of the CNMCAS software and hardware needs additional attention. Additional security features to prevent sabotage of the CNMCAS or alterating data to conceal theft or diversion will be considered. The AGNS staff hopes to show that the checks and balances designed in the system are sufficient to prevent concealment. Computer system security design criteria for the facility are being developed in conjunction with the design of the SCC.

Physical Protection System

The Physical Protection System will provide the following:

- A protected area within which all operations are conducted surrounded by multiple and independent intrusion detection sensors and physical barriers to prevent unauthorized access and to detect any unauthorized access, should it occur. Detections systems are "audited" to limit false alarms during adverse atmospheric conditions, while a satisfactory capability of detecting an intrusion is retained. Ultimately, barriers will be included to delay forced vehicular penetration of the outer perimeter of the protected area.

- Personnel and vehicle access portals equipped with means for identification and search, as appropriate, prior to ingress or egress from the Protected Area.

- A real-time personnel inventory system, including personnel identification based on physical attributes rather than solely on photo badges.

- Closed-circuit TV and motion detection devices for intrusion detection and for surveillance of authorized personnel in restricted areas.

- Protected positions for security personnel from which they can effectively repell an assault.

- Emergency evacuation controls to provide a safe area for searching employees who had access to SNM and to maintain segregation of these employees from those who have had no access to SNM. This will materially reduce the search load and assure a reduced response time.

The existing Physical Protection System was designed to meet the regulatory requirements which were in effect at the end of 1975. An eight-foot chain link fence topped with barbed wire and equipped with motion detection alarms encloses the protected area. Secure Access Passageways (SAP) are installed at the entryways to the protected area and to the two material access areas -- Plutonium Nitrate Storage (PNS) and the Analytical Laboratories (AL). The primary SAP into the PA has personnel monitors for detection of either explosives or metals and an X-ray machine to scan packages. A small SAP is provided to allow access from the non-critical utilities area. Those SAP's leading into Material Access Areas (MAA's) are equipped with both plutonium and metal detectors. Split screen TV cameras at the entrance to the MAA's were installed to allow the picture badge and the person desiring entrance to be compared remotely by a patrolman. The patrolman verifies that the badge picture is for the person requesting entry and determines that the entry is authorized. Then he unlocks the door remotely, so entry can be made. MAA's

are also equipped with CCTV and motion detection alarm devices for surveillance of these areas. Both a Central Alarm Station and a Secondary Alarm Station are included in the existing system.

Testing of the existing system has resulted in the following conclusions:

- Intrusion detection devices for the protected area perimeter should include multiple systems, each employing sensors which measure different physical attributes. Systems should be "anded" to prevent excessive false alarms during inclement weather.

- A remote, immediate alarm assessment capability such as closed-circuit TV is required.

- State-of-the-art explosive detectors' detection failure rates are higher than desirable.

- Canines are potentially more effective than explosive detectors for portal searches.

- Picture badge identification and authorization is satisfactory for the current BNFP population. If the staff were expanded to full strength, the picture badge alone may not be adequate.

- Metal detection is adequate, although safety shoes are a problem.

- Access and egress control points require separate access and egress paths if processing time is to be kept at a reasonable rate.

- State-of-the-art equipment is inadequate for remote personnel or package search.

- Identification and authorization for access or egress requires a system with central programming capability.

Design requirements for generic protected area barriers and alarms with associated personnel and vehicular passageways were developed making liberal use of the results from the excellent work that has been carried out in this field at Sandia. Using these requirements and taking advantage of the existing berm which was required for the BNFP, we have made a preliminary design applicable to the BNFP site. A perspective view of the Personnel Passageway through the Protected Area Boundary is given in Figure 4.

The isolation area between the perimeter fences will be equipped with three different types of monitors with two out of three constituting a valid alarm. A mock-up of a section of the Protected area perimeter with fences has been constructed. The test isolation zone is equipped with the following intrusion detection subsystems:

- Taut Wire Sensors
- Buried Wire Sensors
- Microwave Sensors.

These units have been checked for operability, and they will be subjected to evaluation during the current government fiscal year.

Design requirements for a Vehicle Access Passageway (VAP) have been developed and a conceptual design was prepared. This design is not site-specific, and thus has general applicability. A perspective drawing of the design is shown in Figure 5. A mock-up of the (VAP) which does not include the barriers, the inspection pits, or the personnel passageway was constructed. Operation of the gates, alarms, and CCTV has been verified and tests will be conducted to determine the effect of searches on the flow of vehicles to and from the Protected Area.

Safeguards Coordination Center

The safeguards Coordination Center coordinates the activities of operations, physical security, nuclear materials control and accounting, and others to assure that activities are authorized and are carried out by authorized individuals. It also continuously assesses the status of the entire safeguards system and alerts to any prescribed actions that do not conform to established practice and/or have not received proper authorization for revisions. The SCC will provide an auditable record of activities, procedures, material movement, and personnel access. National and international inspectors may be given these files; and thus with an appropriate response, proliferation from a reprocessing plant can be effectively deterred.

Those areas which are critical to the safeguards efforts are placed under zone control. This system monitors all action by personnel and the process equipment within a specified area. It can interrupt unauthorized operations, alert operation control of procedural discrepancies, or initiate a physical security response. Demonstration of this type of system will be carried out under the "Closed-Loop Control" system which provides for automatic control in key transfer lines and equipment, as well as direct alarm assessment and surveillance by CCTV.

Mock-ups or simulations of these subsystems are being added to the BNFP sequentially, and the combined systems are being tested during simulated plant operation with natural uranium.

The Safeguards Coordination Center is divided into four segments which in aggregate interface all functions associated with operation or control of the facility.

These subsystems which are listed below are subsequently discussed in detail.

- Communications
- Performance Verification
- Zone Operational Control
- Secondary Alarm Station.

COMMUNICATIONS

The communications function is performed through a system of computer interfaces for direct computer-to-computer communications, through hard copy generation of reports for personnel distribution and direct verbal contact with organizational unit representatives. The basic purpose of the communications function is to transmit verified authorizations from the administrative authorities to the executing units. The communications unit also functions to assure the executing unit that all concerned administrative authorities have concurred in granting the authorization.

The basic authorizations required for operation of the facility involve the passage of personnel and materials through an access control point into one of the restricted areas. The routine passages through access control points are dependent on three criteria: (1) meeting the portal search requirements, (2) receiving a valid area authorization, and (3) receiving a valid personnel authorization. The granting of an authorization may require that criteria set by more than one administrative authority be met. When granted, the authorizations are stored in a computer file available to the SCC computer system for search as the requests are generated. The file itself is computer generated from input components from the various administrative authorities. The granting of authorizations is determined by the software which is programmed to consider the multiple requirements for granting any specific authorization. The authorization control concept, when automated, is capable of rapid verification of each individual authorization request.

Performance Verification

A unit responsible for assessing and verifying the overall performance of the safeguards system is part of the Safeguards Coordination Center. The primary verification is that the physical security system is operational and not in an alert mode and that the NMC system is operational with the material accounting within acceptable bounds. The mechanisms for system verification are a combination of communications between computers, surveillance of the Central Alarm Station (CAS) by closed circuit television, a programmed reporting sequence required of the physical security forces, and an on-line check of the physical security computer system. The combination of visual surveillance, reporting, and computer testing of computers allows the safeguards verification unit to ascertain that the physical security system and the NMC system are operating within acceptable performance criteria and that the patrol officers have not been placed under duress.

The performance verification for the NMC computer system will involve determination that the system is not in an alert status. The NMC control unit transmits a status code to the SCC safeguards verification unit on request of the verification unit. This unit also is capable of scanning selected material measurement sensors to determine operability, but it cannot interpret sensor alarms or measurements. A sensor malfunction will be recorded by the verification unit, and the cognizant control officer will be automatically notified of the detected abnormality. The verification of the performance of the physical security system will be performed by CCTV surveillance of the CAS and computer monitoring of the physical security system. The verification

system is also capable of testing and scanning the physical security sensors to determine operability. The detection of an abnormality in a sensor system may initiate a response from the SCC to notify cognizant managerial personnel depending on the significance of the abnormality. As an example, should a scan of the intrusion detection system show that the triplicate sensors in a given area are inoperative and that no alarm condition exists in the physical security central alarm station, the verification unit will not only notify the physical security patrol force but also will initiate immediate notification of physical security management and the process control unit. The detection of such a condition will require that all access to material access areas be denied until the alarm status is resolved. The detection of an abnormal condition in a materials measurement device will also initiate an SCC verification action. The abnormality will first be reported to the NMC control unit, the physical security unit, and the process control center. Should the abnormality not be corrected or authorized within an established time frame, managerial personnel would be notified. The resolution of material measurement abnormalities must be completed before material movements into or out of the affected area will be authorized. The verification unit performs the safeguards system assessment on the basis of programmed performance criteria. The criteria include:

- The physical security sensor surveillance systems are operational
- The physical security system does not indicate an alert status
- The patrol force does not indicate duress
- The NMC system sensors are functional
- The NMC system does not indicate a material discrepancy alert.

Any one or combination of criteria not being met will initiate the SCC verification unit response. The response options include the report sequence previously mentioned, a general alert status activation, or immediate activation of the secondary alarm station and response force notification.

Zone Operations Control

The areas of the facility which, because of the nature of the material contained or operation performed, have been determined to be the most sensitive areas for theft or diversion will have the additional safeguards feature of Zone Operations Control (ZOC). The basic principle added by zone operations control is limitation of the activities which may occur within the area. The control function is applied to those operations which may affect the movement of SNM. The surveillance/detection function of zone control is applied to all accesses into the zone. The control function is limited to authorizing the use of equipment such as valves and pumps by remote operation of electrical devices. The zone operations control center consists of a computer programmed to accept the sequence of events described by the operating procedures approved for the area. The process equipment is designed to allow computer detection of its operational status. The computer compares the determined equipment status with the status required for execution of an authorized procedure. The computer then determines what additional equipment is to be released for operation and what equipment is to be deactivated during the execution of the authorized procedure.

During periods in which no entry into the zone controlled area is authorized, the CAS performs a monitoring surveillance function and the safeguards performance-verification unit performs alarm assessment. The zone is to be fully equipped with intrusion detection and closed-circuit television monitoring equipment. When an authorized entry request is approved by the SCC, the zone control center is activated for that area and the CAS is relieved of that function until the specific area under zone control is returned to an inactive status.

The concepts involved in ZOC have been most fully developed for the BNFP plutonium nitrate storage and loadout system (PNSL). The concept was developed by Sandia Laboratories based on the BNFP design.

The closed-loop control (CLC) concept applied to the BNFP will assure that all operational tasks are performed in a predefined sequence and by the properly authorized individuals. The system will utilize a variety of protective devices coupled with computer checks to rapidly detect unauthorized activities and activate controls, delays, or, where necessary, request response force actions. The CLC system via the ZOC center will:

(1) Accept management directives, data regarding personnel authorized to perform specific plant operations, and the date and time for the operation

(2) Accept the sequence of operational steps and associated criteria

(3) Monitor access and operational event sequence data

(4) Correlate the above data and act on discrepancies.

Through this correlation process the actual activities are compared with predefined authorized procedures. The ZOC can then determine if conditions are normal or if a discrepancy exists. If normal, the operation is allowed to proceed. In the event of a discrepancy, the appropriate error diagnostics are generated and the ZOC operator is alerted with alarm messages. If the discrepancy indicates that unauthorized activities are taking place, then override control signals to process control equipment are sent by ZOC to disable operation of the equipment thereby stopping the operation and a security force response is initiated.

Secondary Alarm Station

The SCC area includes a secondary alarm station. The secondary alarm station provides a command station from which a response may be initiated and directed by the physical security force to delay or deter an adversary action in the event that the central alarm station has been deactivated. The secondary alarm station will contain a duplication of all the physical security communications, surveillance, and alarm assessment equipment essential for providing physical security for the facility. The secondary alarm station is not intended nor equipped to function as a substitute for the Central Alarm Station during routine operations. The activation of the secondary alarm station immediately defines the event as a safeguards emergency and requires that a planned sequence of events and procedures be executed to secure the facility and the materials contained in the facility. The secondary alarm

station can be activated only by the safeguards verification unit based on the previously described activation criteria. When activated, the secondary alarm station may authorize access of response forces into the protected area through the personnel access portal. The access to controlled areas within the protected area will continue to be restricted by the personnel and the area authorization file searches performed by the SCC communications computer system.

The secondary alarm station is manned continuously by a patrol officer stationed in the SCC building. The patrol officer performs the SCC access portal operation in addition to readiness checks of the secondary alarm station. The readiness reporting sequence from the secondary alarm station is a safeguards verification unit requirement.

At present, the AGNS staff has only prepared conceptual designs for the Safeguards Coordination Center including Zone Operations Control of the Plutonium Nitrate Storage Area; the area which, under operating condition, would contain the largest inventory in the Separations Facility of plutonium in a form that might be attractive to antagonists.

The basic information flow diagram for the AGNS organizational structure is shown by Figure 3-1. The organizational structure is shown by functional unit for the purpose of illustrating the communications link provided by the SCC. The diagram does not imply that the communications links shown are the only ones, but rather that the ones shown are the minimum required links for authorization exchange and documentation.

The organizational chart shown in Figure 7 is an example of how the SCC will operate across organizational lines, so that no one division unilaterally controls more than a segment of the Safeguards System.

In addition, design of a mock-up of the Safeguards Coordination Center is well underway utilizing manual interfaces between the center and major components and as safety and operations. Plan view of the mock-up is shown in Figure 8.

As can be seen, the center is divided into two key parts -- Safeguards Operations Center and Program Development Center -- which allows program development work to proceed without interfering with the day-to-day real-time operation of the center.

Figure 9 shows a schematic of the SCC demonstration computer network. At this stage of development, any input from Operations and Security must be fed into the SCC manually.

Conclusions

The layered safeguards provided by the overall concept are developed so that each layer has a distinct safeguards function unaffected by the results of either prior or subsequent safeguards layers. An example typical of the principle is access control. The defeat of the authorization system itself will not guarantee access to a given area. The portal passage criteria must also be defeated or met. Gaining passage through the entry portals does not guarantee access to materials, since NMC, and in critical areas, zone control

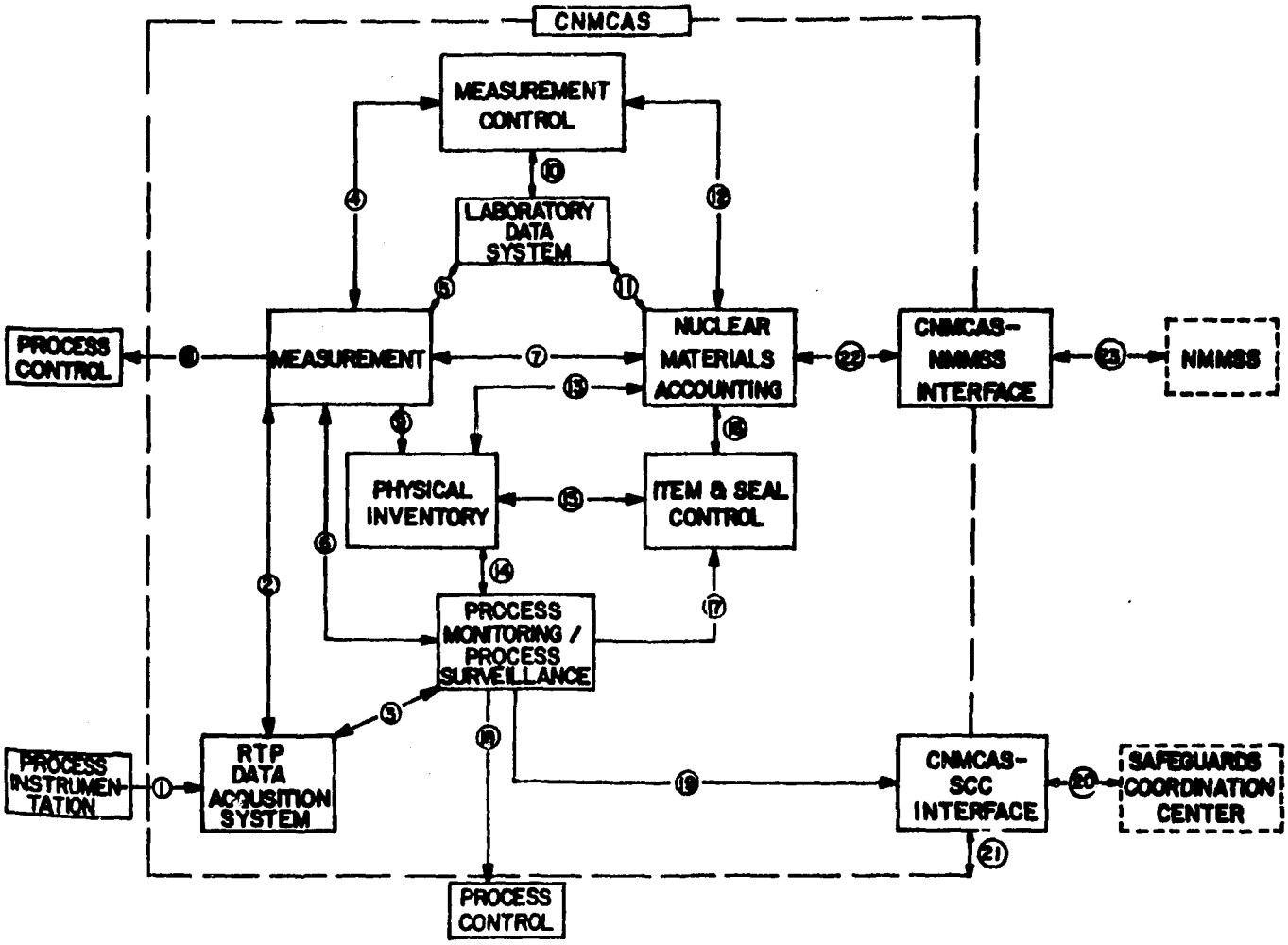
systems must be defeated. The check and balance system also functions for those most likely to be capable of defeating computer systems. The personnel having access to the NMC program and computer cannot gain access to the safeguards computer without at least two-party collusion. The collusion then requires the physical security, zone control, and operations control to be overcome for adversary success. Similarly, those individuals having access to the SCC computer and program do not have access to the authorization processing program or the physical security computer program system.

Should all the computer-based monitoring systems be overcome (i.e., the NMC computer programmed not to recognize a materials inventory change, the SCC computer programmed to accept a falsified area and personnel authorization, and the physical security system programmed not to alarm for area intrusion), the requirements of the physical security system remain formidable barriers to successful theft since all SNM is separated from the uncontrolled areas by at least one entry control portal. An egress from the protected area -- by either a vehicle through the vehicle access portal, or on foot through the personnel access portal -- requires that the individuals be subjected to a search for metal and SNM before egress is permitted. The material access areas are further controlled by an interior access portal imposing the same SNM and metal search criteria. The portal search criteria are not subject to computer interpretation, but direct positive-negative indications to the portal patrolman. The physical security system then provides an independent backup should the computerized systems be defeated.

The foregoing paragraphs illustrate that the computer systems themselves will not, if defeated, guarantee an adversary success. The corollary also holds true; a defeat of the physical search elements of the physical security system will not guarantee adversary success because of the monitoring/surveillance function of the computerized systems. The complementary and overlapping nature of the safeguards systems is intended to provide multiple layers of safeguards, each layer providing an effective element of protection.

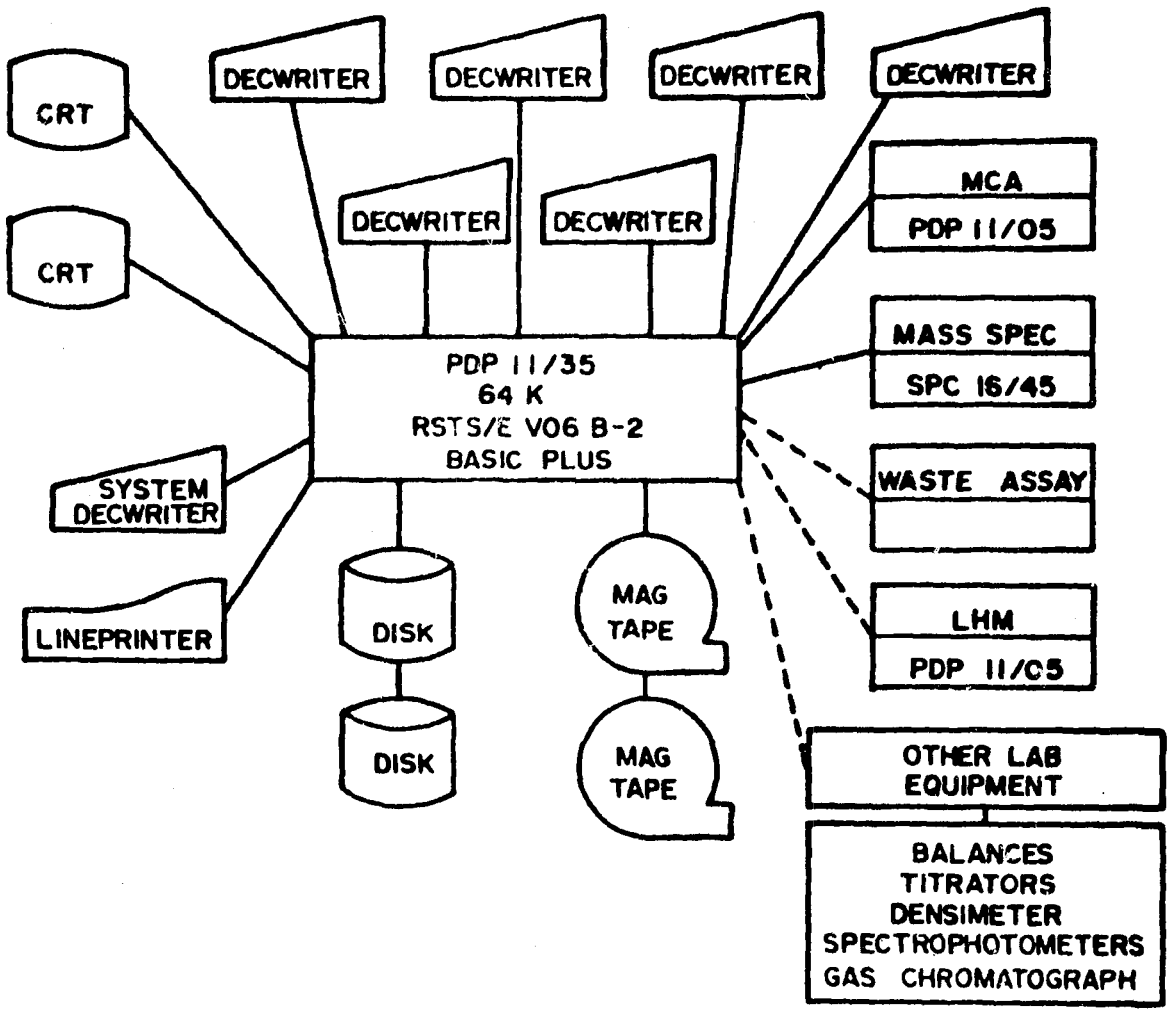
Our tests to date indicate that it does appear to be feasible to meet operational objectives and maintain a high safeguards performance level using these concepts which are being incorporated into the Advanced Safeguards System. Assurance that no primary objectives have been inadvertently eliminated can only be obtained by periodic plant testing as the development proceeds. Final proof can only be established by demonstrating sustained operation of the advanced system with the facility operating on radioactive materials.

Successful demonstration of the Advanced Safeguards System at a reprocessing plant such as the Barnwell Nuclear Fuel Plant would most certainly be a strong deterrent to any group which might otherwise seek to divert special nuclear materials for nonpeaceful purposes and it would discount the claims that SSNM cannot be successfully controlled.



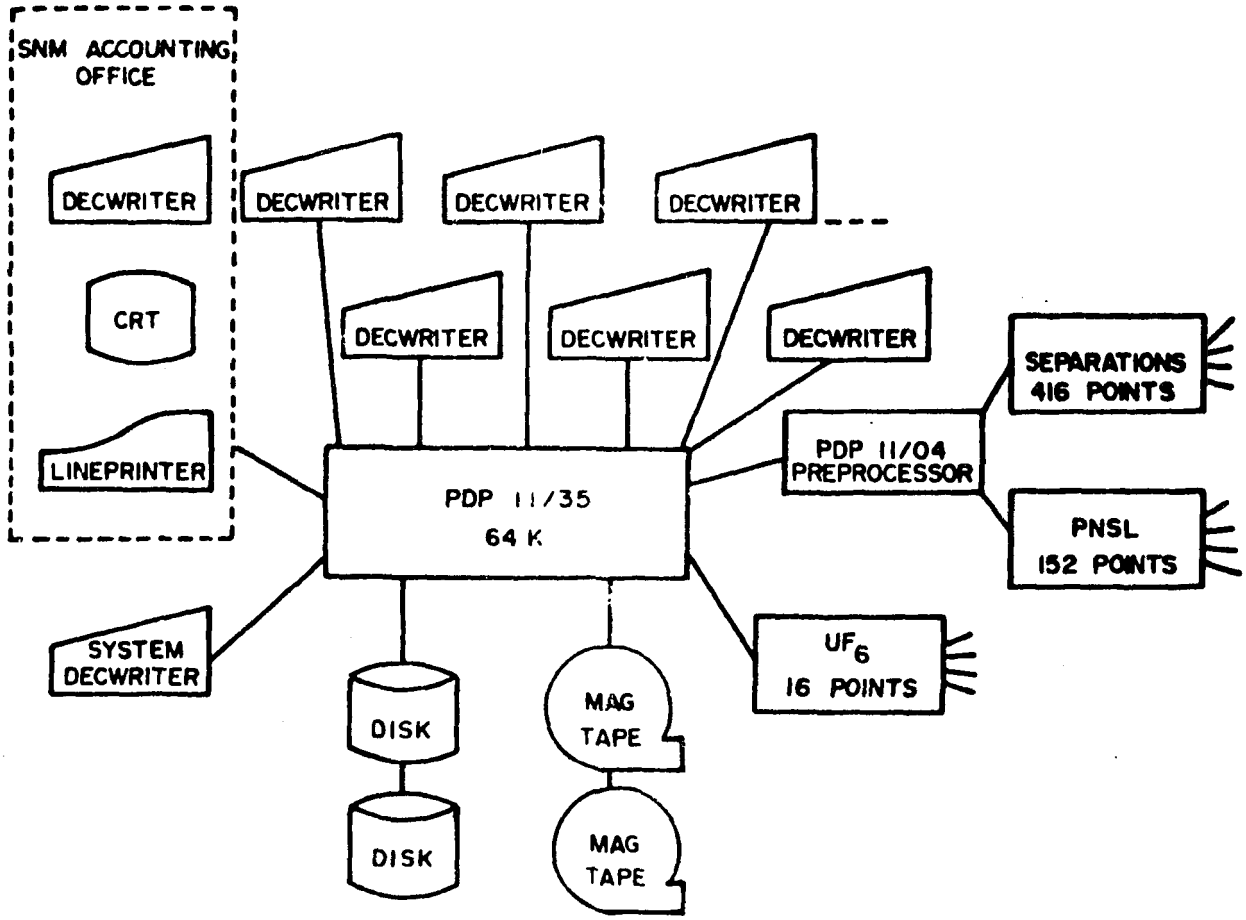
CNMCAS SUBSYSTEM INTERFACES

FIGURE 1



CNMCAS LABORATORY DATA SUBSYSTEM

FIGURE 2



CNMCAS NUCLEAR MATERIALS ACCOUNTING AND CONTROL SYSTEM

FIGURE 3

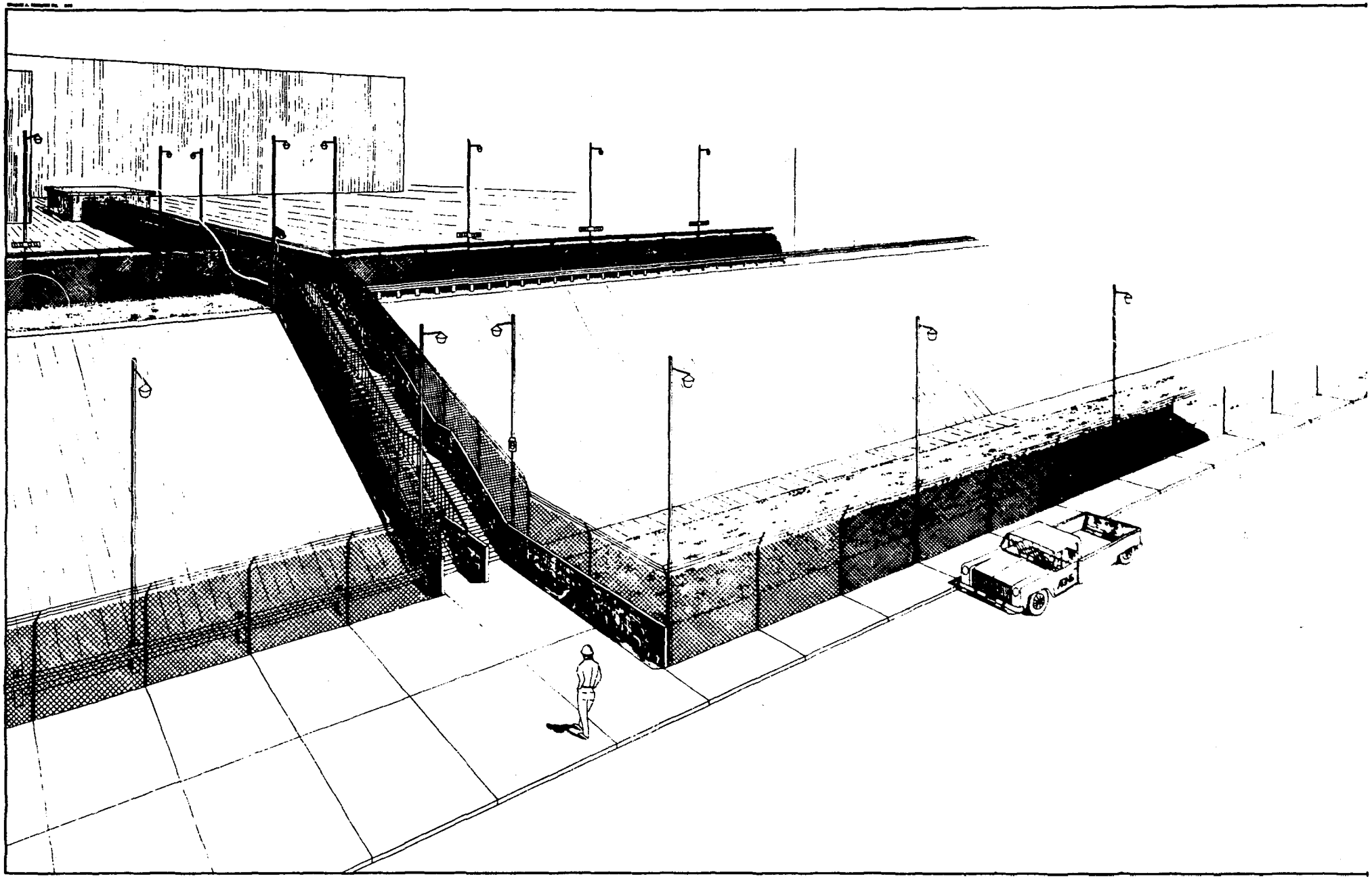


FIGURE 4

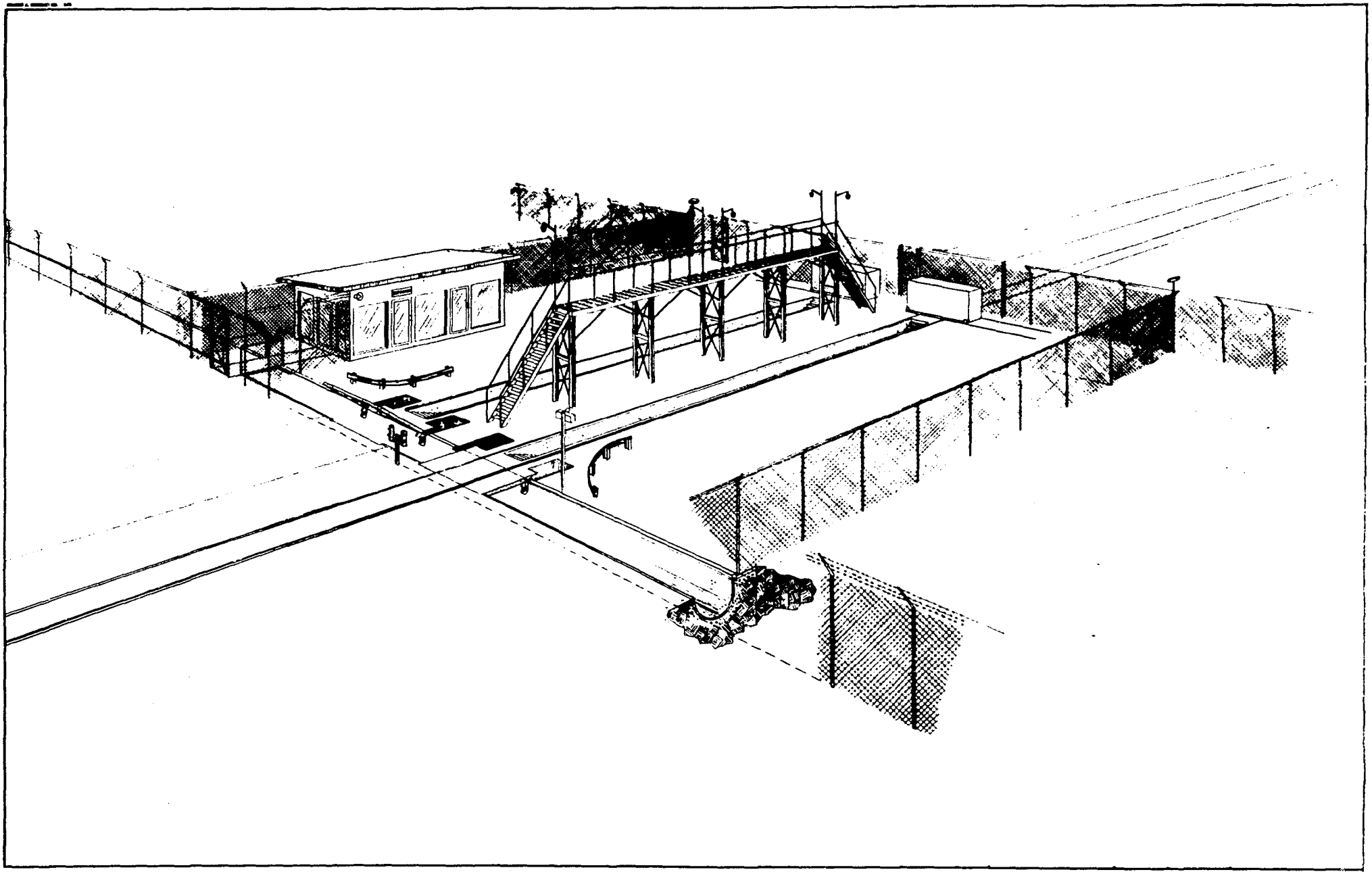
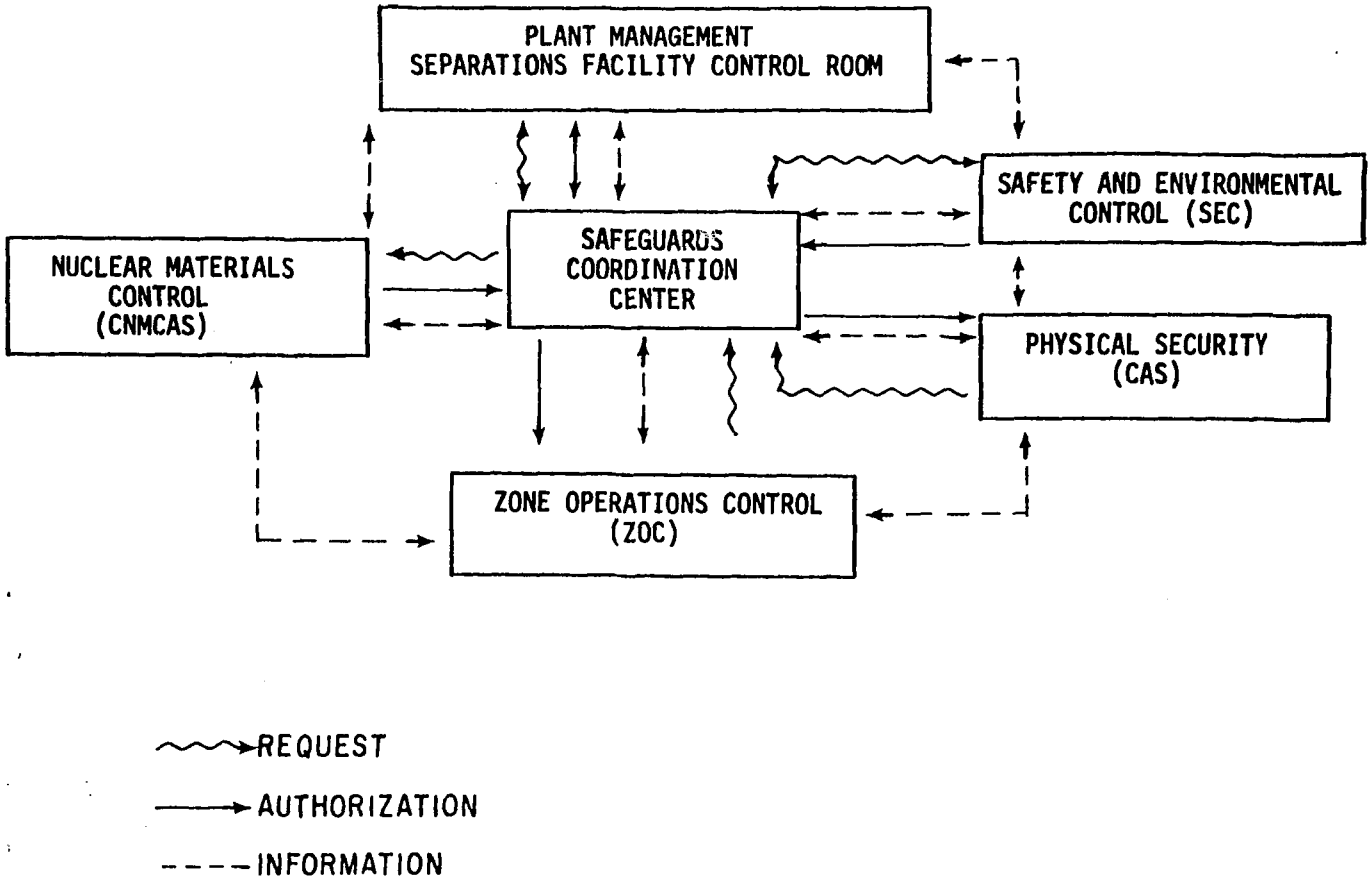


FIGURE 5



FUNCTIONAL DIAGRAM FOR PORPOSED SCC SYSTEM

FIGURE 6

AGNS Organization Chart

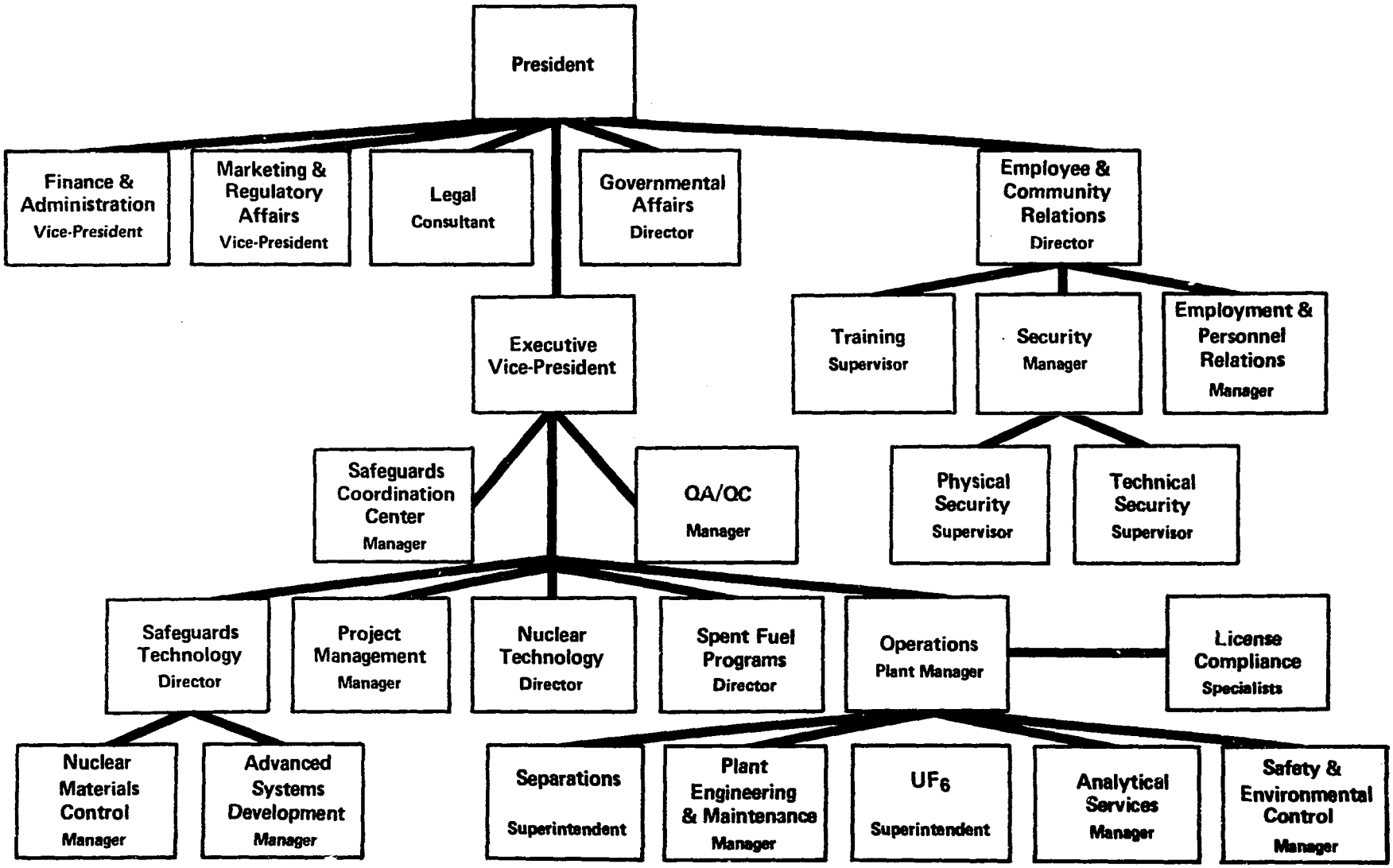
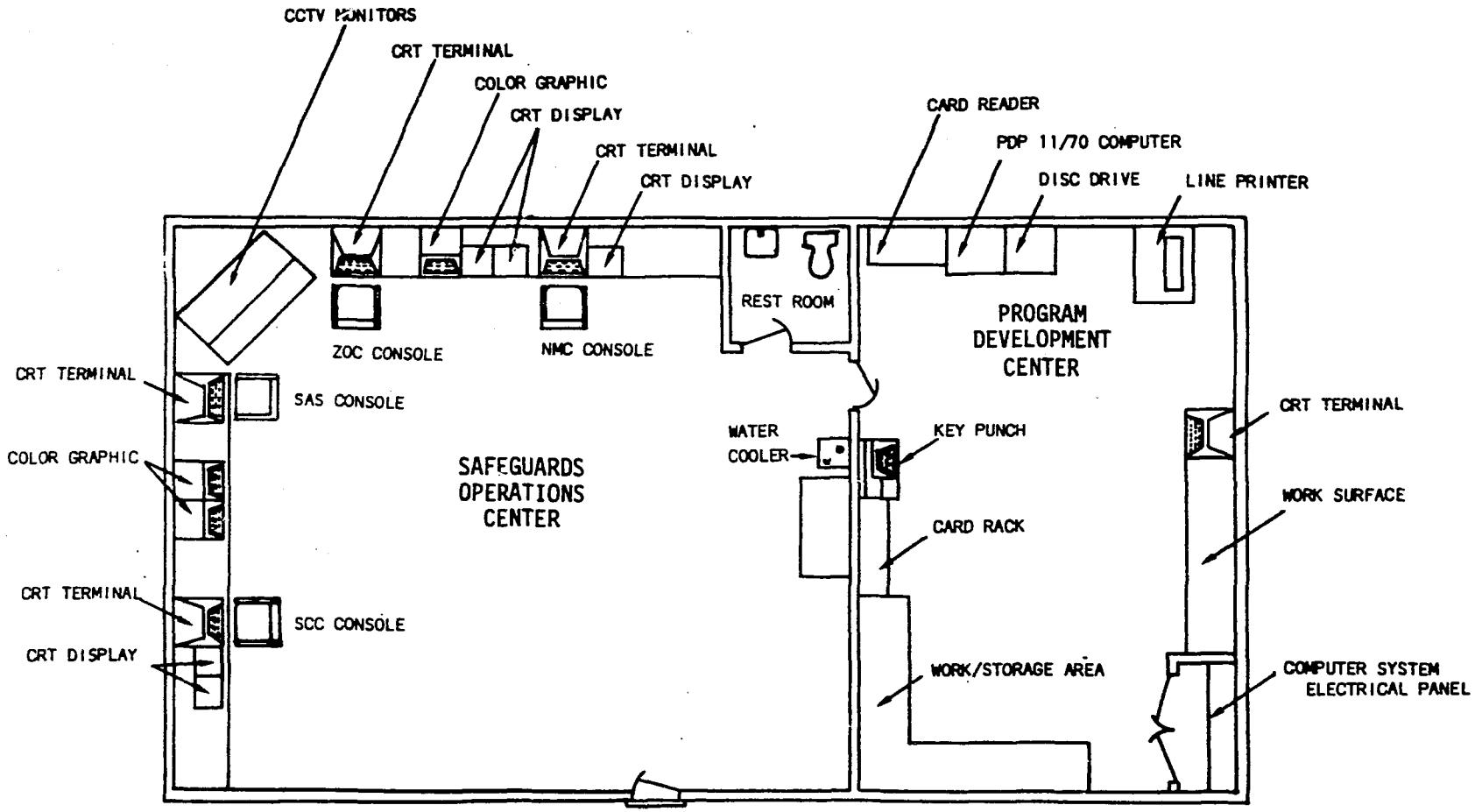
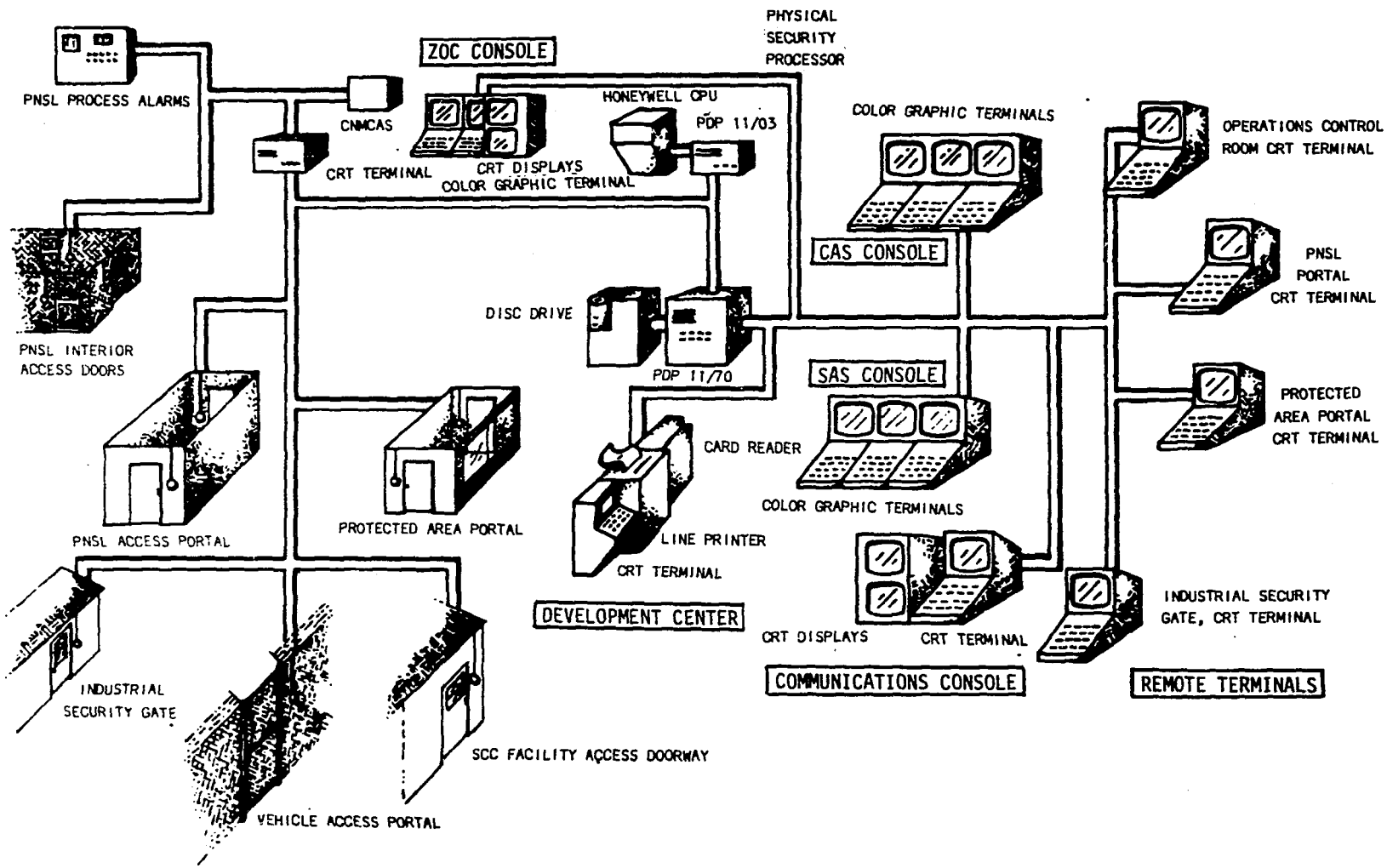


FIGURE 7



SAFEGUARDS COORDINATION CENTER DEMONSTRATION FACILITY FLOOR PLAN

FIGURE 8



SAFEGUARDS COORDINATION CENTER DEMONSTRATION
COMPUTER NETWORK SCHEMATIC

FIGURE 9