MOL.20000321.0284

# OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## ANALYSIS/MODEL COVER SHEET
***Complete Only Applicable Items***

1. QA: QA

Page: 1 of: 89

2. ☒ Analysis ☒ Engineering
☐ Performance Assessment
☐ Scientific

3. ☐ Model ☐ Conceptual Model Documentation
☐ Model Documentation
☐ Model Validation Documentation

4. Title:
Subsurface Repository Integrated Control System Design

5. Document Identifier (including Rev. No. and Change No., if applicable):
ANL-MGR-CS-000001 Rev. 00

6. Total Attachments:
1

7. Attachment Numbers - No. of Pages in Each:
I-73

| | Printed Name | Signature | Date |
|---|---|---|---|
| 8. Originator | D. Craig Randle | D. Craig Randle | 1/5/00 |
| 9. Checker | Jeff T. Pullen | | 1/5/00 |
| 10. Lead/Supervisor | Douglas A. McAffee | Douglas A. McAffee | 1/7/2000 |
| 11. Responsible Manager | Daniel G. McKenzie III | | 1/7/00 |

12. Remarks:

The following TBVs are contained in this document: TBV-406, TBV-407, TBV-409, TBV-411, TBV-415, TBV-417, TBV-1213, TBV-3759.

Primary areas of responsibility for the originator: D. Craig Randle – Coordinated overall preparation of analysis and is the primary author of Secions 6 and 7.

Other contributors to the analysis: Dennis W. Markman – Sections 6.7 and 6.8.

This document supersedes *Subsurface Repository Integrated Control System Design*, BCAC00000-01717-0200-00003 Rev. 00.

# OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
# ANALYSIS/MODEL REVISION RECORD
***Complete Only Applicable Items***

1. Page: 2 of: 89

2. Analysis or Model Title:

Subsurface Repository Integrated Control System Design

3. Document Identifier (including Rev. No. and Change No., if applicable):

ANL-MGR-CS-000001 Rev. 00

| 4. Revision/Change No. | 5. Description of Revision/Change |
|---|---|
| 00 | Initial issue. This document supersedes *Subsurface Repository Integrated Control System Design*, BCAC00000-01717-0200-00003 Rev. 00. |

## CONTENTS

## FIGURES

## TABLES

## ACRONYMS AND ABBREVIATIONS

### Acronyms

| | |
|---|---|
| ANSI | American National Standards Institute |
| ASME | American Society of Mechanical Engineers |
| ATM | asynchronous transfer mode |
| FDDI | fiber distributed data interface |
| HMI | human-machine interface |
| IEEE | Institute of Electrical and Electronics Engineers |
| I&C | instrumentation and control |
| LAN | local area network |
| MGR | monitored geologic repository |
| OMCS | operations monitoring and control system |
| PC | personal computer |
| PLC | programmable logic controller |
| SDD | system description document |
| SSC | systems, structures, and components |
| TBV | to be verified |

### Abbreviations

| | |
|---|---|
| km | kilometer |
| Mbps | megabits per second |

# 1. PURPOSE

The primary purpose of this document is to develop a preliminary high-level functional and physical control system architecture for the potential repository at Yucca Mountain. This document outlines an overall control system concept that encompasses and integrates the many diverse process and communication systems being developed for the subsurface repository design. This document presents integrated design concepts for monitoring and controlling the diverse set of subsurface operations.

The Subsurface Repository Integrated Control System design will be composed of a series of diverse process systems and communication networks. The subsurface repository design contains many systems related to instrumentation and control (I&C) for both repository development and waste emplacement operations. These systems include waste emplacement, waste retrieval, ventilation, radiological and air monitoring, rail transportation, construction development, utility systems (electrical, lighting, water, compressed air, etc.), fire protection, backfill emplacement, and performance confirmation. Each of these systems involves some level of I&C and will typically be integrated over a data communications network throughout the subsurface facility. The subsurface I&C systems will also interface with multiple surface-based systems such as site operations, rail transportation, security and safeguards, and electrical/piped utilities. In addition to the I&C systems, the subsurface repository design also contains systems related to voice and video communications. The components for each of these systems will be distributed and linked over voice and video communication networks throughout the subsurface facility.

The scope and primary objectives of this design analysis are to:

- Identify preliminary system-level functions and interfaces (Section 6.2).

- Examine the overall system complexity and determine how and on what levels the engineered process systems will be monitored, controlled, and interfaced (Section 6.2).

- Develop a preliminary design for the overall Subsurface Repository Integrated Control System functional architecture and graphically depict the operational features of this design through a series of control system functional block diagrams (Section 6.2).

- Develop a physical architecture that presents a viable yet preliminary physical implementation for the Subsurface Repository Integrated Control System functional architecture (Section 6.3).

- Develop an initial concept for an overall subsurface data communications network that can be used to integrate the various control systems comprising the Subsurface Repository Integrated Control System (Section 6.4).

- Develop a preliminary central control room design for the Subsurface Repository Integrated Control System (Section 6.5).

- Identify and discuss the general safety-related issues and design strategies with respect to development of the Subsurface Repository Integrated Control System (Section 6.6)
- Discuss plans for the Subsurface Repository Integrated Control System's response to off-normal operations (Section 6.7).
- Discuss plans and strategies for developing software for the Subsurface Repository Integrated Control System (Section 6.8).

A series of previous analyses have focused primarily on two specific control systems for the subsurface repository, namely the Waste Emplacement System (DIRS 19, DIRS 22, DIRS 23, DIRS 24, and DIRS 25) and the Performance Confirmation System (DIRS 21). There are a number of repository systems for which I&C design work has not yet been initiated, including systems such as fire protection, utilities, and others. As stated earlier, this design analysis is an initial effort to develop a control system design that integrates the entire subsurface repository.

The method used in the development of this document consists in identifying the various subsurface process control/monitoring functions and communications requirements, examining some key implementation strategies, and developing a preliminary conceptual design based on available and emerging technologies. This analysis is an initial effort to develop concepts related to a subsurface facility-wide process monitoring, control, and communications system. As such, the methodology of this analysis combines examination of the System Description Documents (SDDs), evaluation and identification of existing systems and technologies, and discussion and preliminary analysis of key issues and ideas related to integrated subsurface monitoring, control, and communications.

The general approach in developing this analysis is to:

- Identify and review the key design input source documents (the SDDs).
- Perform preliminary analyses and design activities.
- Summarize key findings.
- Provide recommendations.

This document supports the development of Section 2.0 of the SDDs cited in Section 6.2.2 of this analysis which, in turn, will support the Site Recommendation Consideration Report.

# 2. QUALITY ASSURANCE

The Subsurface Repository Integrated Control System, which is part of the Monitored Geologic Repository (MGR) Operations Monitoring and Control System, has been classified in accordance with QAP-2-3, *Classification of Permanent Items,* and found to be quality affecting (DIRS 31). This design activity has been evaluated in accordance with QAP-2-0, *Conduct of Activities* (DIRS 28), and has been determined to be quality affecting subject to the requirements of the *Quality Assurance Requirements and Description* (DIRS 29). This design analysis has been prepared in accordance with an approved development plan (DIRS 71).

## 3. COMPUTER SOFTWARE AND MODEL USAGE

This section is not applicable. There are no applicable computer software or models that are used in support of this analysis.

## 4. INPUTS

### 4.1 DATA AND PARAMETERS

This section is not applicable. There are no numerical, scientific, or performance assessment values that are applicable to this analysis.

### 4.2 CRITERIA

The criteria identified in this section are the only applicable portions of the SDDs related to the preliminary design concepts presented in this analysis. Other SDD criteria will become applicable at more refined levels of I&C system design, but do not impact the designs presented herein.

4.2.1 The Performance Confirmation Emplacement Drift Monitoring System shall monitor emplaced waste packages, emplacement drift environmental conditions, and emplace/recover drift test coupons. Refer to the *Performance Confirmation Emplacement Drift Monitoring System Description Document* (DIRS 5), Volume I, Sections 1.1.1 through 1.1.5, p. 6; (used in Section 6.2.2.4).

4.2.2 The Waste Emplacement System shall receive loaded waste packages, transport waste packages to the subsurface, emplace waste packages, provide remote control capability for waste transport, emplacement, recovery and removal operations, provide remote visual surveillance of transport and emplacement operations, and interface with other MGDS systems. Refer to the *Waste Emplacement System Description Document* (DIRS 2), Volume I, Sections 1.1.1 through 1.1.7, p. 7; (used in Section 6.2.2.2).

4.2.3 The Subsurface Ventilation System shall generate and control air flow in development and emplacement areas, control air temperature in development and emplacement areas, maintain air quality in development and emplacement areas, provide air cleanup and filtration in development and emplacement areas, limit radioactive contaminant dispersion, control human access to emplacement areas, provide monitored status of system operation, control the spread of combustion products due to fire, and provide operation parameters and air-related environmental data to facility control systems. Refer to the *Subsurface Ventilation System Description Document* (DIRS 1), Volume I, Sections 1.1.1 through 1.1.7, 1.1.10, and 1.1.11, p. 6; (used in Section 6.2.2.8).

4.2.4 The Waste Retrieval System shall retrieve emplaced waste packages under normal and abnormal conditions. Refer to the *Waste Retrieval System Description Document* (DIRS 6), Volume I, Sections 1.1.1 through 1.1.4, p. 7; (used in Section 6.2.2.6).

4.2.5 The Backfill Emplacement System shall transport backfill material to the subsurface facility and place backfill material in the emplacement drifts. Refer to the *Backfill*

*Emplacement System Description Document* (DIRS 7), Volume I, Sections 1.1.2 and 1.1.3, p. 6; (used in Section 6.2.2.7).

4.2.6 The Ground Control System shall monitor the behavior of ground control components and the host rock. Refer to the *Ground Control System Description Document* (DIRS 4), Volume I, Section 1.1.3, p. 6; (used in Section 6.2.2.14).

4.2.7 The Performance Confirmation Data Acquisition/Monitoring System shall monitor, test, and collect data on repository excavation, borehole parameters, and waste package parameters. Refer to the *Performance Confirmation Data Acquisition/Monitoring System Description Document* (DIRS 8), Volume I, Sections 1.1.4 and 1.1.5, p. 8; (TBV-407); (used in Section 6.2.2.5).

4.2.8 The MGR Operations Monitoring and Control System shall provide for the centralized monitoring and control of essential activities and safety-related systems throughout the subsurface repository. Refer to the *Monitored Geologic Repository Operations Monitoring and Control System Description Document* (DIRS 3), Volume I, Sections 1.1.1, 1.1.2, 1.1.3, 1.1.6 through 1.1.14, 1.1.16, and 1.1.17, pp. 8-9; (TBV-3759). The individual system functions are listed below by section and page number of this document insofar as they apply to subsurface operational activities:

- From a central control room, the system monitors, controls, and interfaces, as necessary, with all operating subsurface systems. Refer to Section 1.1.1, p. 8; (used in Section 6.5).

- The system provides supervisory control of the subsurface ventilation system under normal, emergency, and "off-normal" conditions. Refer to Section 1.1.2, p. 8; (used in Section 6.2.2.8).

- The system provides supervisory control of the subsurface utilities such as power distribution. Refer to Section 1.1.3, p. 8; (used in Sections 6.2.2.12 and 6.2.2.13).

- The system controls the orderly shutdown of subsurface systems. Refer to Section 1.1.6, p. 8; (used in Section 6.7.3).

- The system monitors the status of the subsurface operational safety systems involving waste emplacement. Refer to Section 1.1.7, p. 8; (used in Sections 6.2.2.2 and 6.2.2.3).

- The system monitors and controls safety systems, and responds to and recovers from off-normal events and Category I and II Design Basis Events. Refer to Section 1.1.8, p. 8; (used in Sections 6.2.2.1 and 6.7.1).

- The system monitors and controls operational startup of the subsurface facility following a routine or off-normal operations shutdown. Refer to Section 1.1.9, p. 8; (used in Sections 6.2.2.1 and 6.7.3).

- The system provides alarms when off-normal conditions are detected by systems providing data to it. Refer to Section 1.1.10, p. 8; (used in Sections 6.2.2.1 and 6.7.3).

- The system monitors subsurface equipment performance and diagnostics to ensure it is operating within the established design limits. Refer to Section 1.1.11; p. 8; (used in Section 6.2.2.1).

- The system interfaces with other MGR systems to exchange information for integrated control and monitoring of subsurface operations. Refer to Section 1.1.12, p. 8; (used in Section 6.2.2.1).

- The system provides a centralized capability for generating, accessing, monitoring, processing, and managing subsurface voice, audio, video, and data communications. Refer to Section 1.1.13, p. 8; (used in Section 6.2.2.11).

- The system provides monitoring, tracking, and trending of radioactive effluents which may be accidentally released to the subsurface environment. Refer to Section 1.1.14, p. 9; (used in Section 6.2.2.5).

- The system monitors, reports, and stores subsurface environmental data. Refer to Section 1.1.16, p. 9; (used in Section 6.2.2.9).

- The system completes, by remote control, all waste emplacement and performance confirmation operations. Refer to Section 1.1.17, p. 9; (used in Sections 6.2.2.2 and 6.2.2.4).

4.2.9 The MGR Operations Monitoring and Control System shall initiate local and remote alarms in response to subsurface radiation hazards. Refer to the *Monitored Geologic Repository Operations Monitoring and Control System Description Document* (DIRS 3), Volume I, Section 1.2.1.9, p. 10; (used in Section 6.2.2.9).

4.2.10 The MGR Operations Monitoring and Control System shall monitor and initiate an alarm for low differential pressure between all emplacement drifts and the related emplacement drift turnouts. Refer to the *Monitored Geologic Repository Operations Monitoring and Control System Description Document* (DIRS 3), Volume I, Section 1.2.1.11, p. 11; (used in Section 6.2.2.8).

4.2.11 The MGR Operations Monitoring and Control System shall monitor the status of the emplacement drift isolation doors and initiate alarms to warn control room operators if personnel attempt to enter the emplacement drifts with a high radiation potential. Refer to the *Monitored Geologic Repository Operations Monitoring and Control System Description Document* (DIRS 3), Volume I, Section 1.2.1.15, p. 11; (used in Section 6.2.2.2).

4.2.12 The MGR Operations Monitoring and Control System shall provide for simultaneous real-time monitoring and control of all remote operations. Refer to the *Monitored*

*Geologic Repository Operations Monitoring and Control System Description Document* (DIRS 3), Volume I, Section 1.2.1.22, p. 12; (used in Section 6.2.2.1).

4.2.13 The MGR Operations Monitoring and Control System shall provide backup data storage of critical operational monitoring, alarm status, environmental conditions, and safety-related data. Refer to the *Monitored Geologic Repository Operations Monitoring and Control System Description Document* (DIRS 3), Volume I, Section 1.2.1.23, p. 12; (used in Section 6.2.2.1).

4.2.14 The MGR Operations Monitoring and Control System shall have the capability for hardware and software expansion with minimum impact on existing hardware, applications software and the real-time operating system. Refer to the *Monitored Geologic Repository Operations Monitoring and Control System Description Document* (DIRS 3), Volume I, Section 1.2.1.27, p. 12; (used in Sections 6.2.2.1 and 6.3.1.10).

4.2.15 The MGR Operations Monitoring and Control System shall provide diversity, separation, or other means to reduce the likelihood of common-cause failures of redundant controls and status indications important to safety systems. Refer to the *Monitored Geologic Repository Operations Monitoring and Control System Description Document* (DIRS 3), Volume I, Section 1.2.2.1.9, p. 17; (used in Section 6.3.1.4).

4.2.16 The MGR Operations Monitoring and Control System shall provide the capability to monitor area radiation levels (direct radiation, gaseous, and airborne particulate) during normal operations and credible design basis events. Refer to the *Monitored Geologic Repository Operations Monitoring and Control System Description Document* (DIRS 3), Volume I, Section 1.2.2.1.17, p. 18; (used in Section 6.2.2.9).

4.2.17 The MGR Operations Monitoring and Control System shall initiate a radiation alarm system to warn of significant increases in radiation levels and concentrations of radioactive materials in the air. Refer to the *Monitored Geologic Repository Operations Monitoring and Control System Description Document* (DIRS 3), Volume I, Section 1.2.2.1.19, p. 18; (used in Section 6.2.2.9).

4.2.18 The MGR Operations Monitoring and Control System shall be designed such that a single failure of the redundant communications between the master control unit and the RTU will not affect monitoring and remote control of ITS operations. Refer to the *Monitored Geologic Repository Operations Monitoring and Control System Description Document* (DIRS 3), Volume I, Section 1.2.2.1.20, p. 18; (used in Sections 6.3.1.4 and 6.6.2.1).

4.2.19 The MGR Operations Monitoring and Control System shall monitor and alarm for low differential pressure between the emplacement and development areas. Refer to the *Monitored Geologic Repository Operations Monitoring and Control System Description Document* (DIRS 3), Volume I, Section 1.2.2.1.21, p. 18; (used in Section 6.2.2.8).

4.2.20 The Subsurface Fire Protection System shall provide personnel and system, structure, and component protection from identified in-situ and transient fire hazards, and from the effects of fire suppression agents. Refer to the *Subsurface Fire Protection System*

*Description Document* (DIRS 9), Volume I, Section 1.1.1, p. 7; (used in Section 6.2.2.10).

4.2.21 The Subsurface Fire Protection System shall provide the means to control, prevent propagation, and extinguish subsurface fires. Refer to the *Subsurface Fire Protection System Description Document* (DIRS 9), Volume I, Section 1.1.2, p. 7; (used in Section 6.2.2.10).

4.2.22 The Subsurface Fire Protection System shall provide means for the detection and annunciation of subsurface fires. Refer to the *Subsurface Fire Protection System Description Document* (DIRS 9), Volume I, Section 1.1.3, p. 7; (used in Section 6.2.2.10).

4.2.23 The Subsurface Fire Protection System shall distribute and provide the means to deliver fire suppression in the subsurface areas. Refer to the *Subsurface Fire Protection System Description Document* (DIRS 9), Volume I, Section 1.1.4, p. 7; (used in Section 6.2.2.10).

4.2.24 The Subsurface Fire Protection System shall provide the means to detect, control, and mitigate credible unplanned subsurface explosion hazards. Refer to the *Subsurface Fire Protection System Description Document* (DIRS 9), Volume I, Section 1.1.5, p. 7; (used in Section 6.2.2.10).

4.2.25 The Subsurface Fire Protection System shall provide occupant notification of subsurface fire emergency/evacuation conditions. Refer to the *Subsurface Fire Protection System Description Document* (DIRS 9), Volume I, Section 1.1.6, p. 7; (used in Section 6.2.2.10).

4.2.26 The Subsurface Electrical Distribution System shall distribute electrical power during construction, operation, caretaker and closure phases of the repository. Refer to the *Subsurface Electrical Distribution System Description Document* (DIRS 10), Volume I, Section 1.1.1, p. 7; (used in Section 6.2.2.12).

4.2.27 The Subsurface Electrical Distribution System shall monitor incoming power quality, system operating parameters, and equipment status. Refer to the *Subsurface Electrical Distribution System Description Document* (DIRS 10), Volume I, Section 1.1.3, p. 7; (used in Section 6.2.2.12).

4.2.28 The Subsurface Electrical Distribution System shall provide normal and standby power. Refer to the *Subsurface Electrical Distribution System Description Document* (DIRS 10), Volume I, Section 1.1.5, p. 7; (used in Section 6.2.2.12).

4.2.29 The Subsurface Electrical Distribution System shall distribute and transform electrical power for the subsurface facility. Refer to the *Subsurface Electrical Distribution System Description Document* (DIRS 10), Volume I, Section 1.1.6, p. 7; (used in Section 6.2.2.12).

4.2.30 The Subsurface Electrical Distribution System shall provide lighting, grounding, and lightning protection for the subsurface facility. Refer to the *Subsurface Electrical Distribution System Description Document* (DIRS 10), Volume I, Section 1.1.7, p. 7; (used in Section 6.2.2.12).

4.2.31 The Subsurface Excavation System shall excavate the subsurface openings necessary to gain access and conduct operations in the underground environment for waste emplacement and associated operations. Refer to the *Subsurface Excavation System Description Document* (DIRS 11), Volume I, Section 1.1.1, p. 8; (used in Section 6.2.2.14).

## 4.3 CODES AND STANDARDS

4.3.1 American Society of Mechanical Engineers (ASME)

| | |
|---|---|
| ASME NQA-1-1997 | *Quality Assurance Program Requirements for Nuclear Facility Applications* (1997) (DIRS 36) |

4.3.2 Institute of Electrical and Electronics Engineers (IEEE)

| | |
|---|---|
| IEEE Std 7-4.3.2-1993 | *IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations* (1993) (DIRS 37) |
| IEEE Std 352-1987 | *IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Protection Systems* (1987) (DIRS 38) |
| IEEE Std 577-1976 | *IEEE Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Power Generating Stations* (1976) (DIRS 39) |
| IEEE Std 603-1991 | *IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations* (1991) (DIRS 40) |
| IEEE Std 730-1998 | *IEEE Standard for Software Quality Assurance Plans* (1998) (DIRS 41) |
| IEEE Std 730.1-1995 | *IEEE Guide for Software Quality Assurance Planning* (1995) (DIRS 42) |
| IEEE Std 828-1990 | *IEEE Standard for Software Configuration Management Plans* (1990) (DIRS 43) |
| ANSI/IEEE Std 829-1983 | *IEEE Standard for Software Test Documentation* (1983) (DIRS 44) |

| | |
|---|---|
| IEEE Std 830-1993 | *IEEE Recommended Practice for Software Requirements Specifications* (1993) (DIRS 45) |
| IEEE Std 1008-1987 | *IEEE Standard for Software Unit Testing* (1987) (DIRS 46) |
| IEEE Std 1012-1986 | *IEEE Standard for Software Verification and Validation Plans* (1986) (DIRS 47) |
| IEEE Std 1016-1987 | *IEEE Recommended Practice for Software Design Descriptions* (1987) (DIRS 48) |
| IEEE Std 1023-1988 | *IEEE Guide for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations* (1988) (DIRS 49) |
| IEEE Std 1028-1988 | *IEEE Standard for Software Reviews and Audits* (1988) (DIRS 50) |
| IEEE Std 1042-1987 | *IEEE Guide to Software Configuration Management* (1987) (DIRS 51) |
| IEEE Std 1059-1993 | *IEEE Guide for Software Verification and Validation Plans* (1993) (DIRS 52) |
| IEEE Std 1063-1987 | *IEEE Standard for Software User Documentation* (1987) (DIRS 53) |
| IEEE Std 1074-1995 | *IEEE Standard for Developing Software Life Cycle Processes* (1995) (DIRS 54) |

### 4.3.3 U. S. Nuclear Regulatory Commission

| | |
|---|---|
| NUREG/CR-6101 | *Software Reliability and Safety in Nuclear Reactor Protection Systems* (November 1993) (DIRS 56) |
| NUREG/CR-6263 | *High Integrity Software for Nuclear Power Plants* (June 1995) (DIRS 57) |
| NUREG/CR-6278 | *Survey of Industry Methods for Producing Highly Reliable Software* (November 1994) (DIRS 58) |
| NUREG/CR-6294 | *Design Factors for Safety-Critical Software* (December 1994) (DIRS 59) |

| | |
|---|---|
| NUREG/CR-6421 | *A Proposed Acceptance Process for Commercial Off-the-Shelf (COTS) Software in Reactor Applications* (March 1996) (DIRS 60) |
| NUREG/CR-6463 Rev. 1 | *Review Guidelines for Software Languages for Use in Nuclear Power Plant Safety Systems* (October 1997) (DIRS 61) |
| NUREG/CR-6465 | *Development of Tools for Safety Analysis of Control Software in Advanced Reactors* (April 1996) (DIRS 62) |
| Regulatory Guide 1.152 Rev. 1 | *Criteria for Digital Computers in Safety Systems of Nuclear Power Plants* (January 1996) (DIRS 63) |
| Regulatory Guide 1.153 Rev. 1 | *Criteria for Safety Systems* (June 1996) (DIRS 64) |
| Regulatory Guide 1.168 | *Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants* (September 1997) (DIRS 65) |
| Regulatory Guide 1.169 | *Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants* (September 1997) (DIRS 66) |
| Regulatory Guide 1.170 | *Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants* (September 1997) (DIRS 67) |
| Regulatory Guide 1.171 | *Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants* (September 1997) (DIRS 68) |
| Regulatory Guide 1.172 | *Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants* (September 1997) (DIRS 69) |
| Regulatory Guide 1.173 | *Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants* (September 1997) (DIRS 70) |

## 5. ASSUMPTIONS

5.1 The Subsurface Emplacement Transportation System shall provide remote rail switching throughout the subsurface facility (used in Section 6.2.2.3). It is expected that this system function will be included in the forthcoming *Subsurface Emplacement Transportation System Description Document* (TBV-406) (DIRS 12).

5.2 The Subsurface Emplacement Transportation System shall provide train collision and derailment protection throughout the subsurface facility (used in Section 6.2.2.3). It is expected that this system function will be included in the forthcoming *Subsurface Emplacement Transportation System Description Document* (TBV-406) (DIRS 12).

5.3 The Subsurface Emplacement Transportation System shall provide an electrification system to power rail vehicles throughout the subsurface facility (used in Section 6.2.2.3). It is expected that this system function will be included in the forthcoming *Subsurface Emplacement Transportation System Description Document* (TBV-406) (DIRS 12).

5.4 The Subsurface Compressed Air System shall provide for the distribution of compressed air throughout subsurface areas (used in Section 6.2.2.13). It is expected that this system function will be included in the forthcoming *Subsurface Compressed Air System Description Document* (TBV-409) (DIRS 13).

5.5 The Subsurface Water Distribution System shall provide for the distribution of both potable and non-potable water throughout subsurface areas for underground construction and development activities (used in Section 6.2.2.13). It is expected that this system function will be included in the forthcoming *Subsurface Water Distribution System Description Document* (TBV-415) (DIRS 15).

5.6 The Subsurface Water Collection/Removal System shall provide for the collection of water from subsurface areas (used in Section 6.2.2.13). It is expected that this system function will be included in the forthcoming *Subsurface Water Collection/Removal System Description Document* (TBV-411) (DIRS 14).

5.7 The Subsurface Water Collection/Removal System shall provide for the removal of collected water from the subsurface (used in Section 6.2.2.13). It is expected that this system function will be included in the forthcoming *Subsurface Water Collection/Removal System Description Document* (TBV-411) (DIRS 14).

5.8 The Subsurface Water Collection/Removal System shall provide for the treatment of water removed from the subsurface (used in Section 6.2.2.13). It is expected that this system function will be included in the forthcoming *Subsurface Water Collection/Removal System Description Document* (TBV-411) (DIRS 14).

5.9 The Muck Handling System shall provide for the transportation of excavated rock from subsurface areas to the surface (used in Section 6.2.2.14). It is expected that this system function will be included in the forthcoming *Muck Handling System Description Document* (TBV-417) (DIRS 16).

5.10 The Subsurface Development Transportation System shall provide for rail transportation to and from development throughout the subsurface facility (used in Section 6.2.2.14). It is expected that this system function will be included in the forthcoming *Subsurface Development Transportation System Description Document* (TBV-1213) (DIRS 17).

# 6. ANALYSIS

## 6.1 INTRODUCTION

This analysis discusses preliminary design concepts for a subsurface facility-wide integrated monitoring and control system, known as the Subsurface Repository Integrated Control System. Functions related to subsurface control are identified primarily from the SDDs listed in Section 6.2.2. These functions are organized systematically in functional block diagrams (Section 6.2). These diagrams show the basic data flow and system separation of subsurface activities and functions. These functions are organized in a logical manner to be implemented by the equipment shown in the physical architecture diagrams (Section 6.3). Both the functional and physical diagrams show a control hierarchy in a layered setup. In the functional block diagrams, these layers separate the high-level functions, based on the SDD descriptions, from lower level sub-functions. The physical architecture diagrams depict the control and monitoring hierarchy and show the different levels of control. The scope of this document does not include site-wide integration.

The data communications system, which correlates to the physical architecture, is discussed in Section 6.4. A preliminary control room layout design for the Subsurface Repository Integrated Control System is presented in Section 6.5. Section 6.6 discusses safety-related issues pertaining to the Subsurface Repository Integrated Control System design. A plan for addressing off-normal operations is given in Section 6.7. Section 6.8 discusses plans and strategies for developing and managing software for the Subsurface Repository Integrated Control System.

## 6.2 SUBSURFACE REPOSITORY INTEGRATED CONTROL SYSTEM FUNCTIONAL ARCHITECTURE

This section presents a preliminary functional architecture for the Subsurface Repository Integrated Control System. It presents a series of control system functional block diagrams that correlate key high-level functions identified in the SDDs to specific equipment and components being designed by the Repository Subsurface Design Group. In essence, the functional block diagrams map SDD functions into the individual systems, structures, and components (SSCs) being developed to satisfy subsurface repository operations.

The preliminary functional block diagrams for the MGR systems are graphically represented by the group of figures located at the end of this section (see Figures 1 through 18). Each figure depicts an eight-level vertical hierarchy of I&C or communications-related SSCs located throughout the repository. Each level (or layer) contains functional elements that tend to become more specific or specialized in moving from top to bottom through the hierarchical structure. The functional block diagrams identify primary system-level functions and interfaces, and identify on what levels these systems will be controlled and integrated. They also provide an indication of the overall size and complexity involved in developing an integrated control system for the subsurface repository.

### 6.2.1 Overview of Control System Functional Block Diagrams

The conceptual and graphical format for the functional block diagram figures appearing in this design analysis were adapted in part from a methodology for developing a logical hierarchical architecture developed by the National Institute of Standards and Technology. The National Institute of Standards and Technology methodology has been applied to the design of various complex systems including automated control systems in the mining industry. Refer to the *Mining Automation Real-Time Control system Architecture Standard Reference Model (MASREM)* (DIRS 18) for more information regarding the National Institute of Standards and Technology hierarchical structuring technique.

The development strategy for organizing the functional architecture presented in Figures 1 through 18 was to correlate items at the system level of the hierarchy with the process systems related to the subsurface operations of the MGR outlined in the SDDs. On each control system functional block diagram is one or more double-lined blocks. A double-lined block indicates that its depicted lower level hierarchical tree is both graphically and functionally rooted at this point.

The elements appearing on the site, facility, system, and primary function levels graphically represents all of the peer system interfaces and functional subsystems described in the various SDDs shown on the figures as double-lined blocks. Usually, the block elements on the site, facility, and system levels carry their corresponding SDD reference number in the upper right-hand corner. The various process elements linked together throughout the remaining equipment/subsystem, operation, monitoring/control, and device levels of the hierarchy denote functional SSCs described in various design analyses, technical reports, or draft documents.

The hierarchical levels or layers of the functional design architecture for the subsurface repository are defined and described in general in this section. Also noted here are examples of the types of items that appear on each layer and how each layer interfaces with the layers above and below it.

The "Site Level" identifies SDD systems that have a functional range extending throughout the MGR. These site-wide SDDs encompass both surface and subsurface functions and operations. These SDD systems interface primarily with the subsurface portion of the MGR Operations Monitoring and Control System (OMCS), known as the Subsurface Repository Integrated Control System, appearing on the facility level.

The "Facility Level" identifies SDD systems whose I&C-related functions impact the subsurface facility as a whole and interface directly with site-level SDD systems. The primary element on this level is the subsurface portion of the MGR OMCS, known as the Subsurface Repository Integrated Control System. This system will functionally serve in a supervisory capacity for the entire subsurface repository and, as such, will coordinate, monitor, and control all key operational, performance, and safety-related activities.

The "System Level" identifies each subsurface SDD system that includes I&C-related functions and shows primary interfaces to facility and site-level SDD systems. Key functions for each system-level SDD systems are represented on the primary function level below.

The "Primary Function Level" contains the main or primary I&C-related functions allocated to each of the SDD systems located on the system level. Where available, these items are taken directly from the "System Functions" section (Section 1.1) of each SDD. The SDD subsection number for each function appears in the lower right-hand corner of the block element. Not all functions identified in the SDDs are depicted in the functional block diagrams. Only the primary functions logically related to the Subsurface Repository Integrated Control System are considered in this analysis. Also, since not all subsurface-related SDDs have been completed to date, appropriate TBVs have been assigned for tracking purposes. The primary functions can, in turn, be described in terms of groups of functionally related equipment or subsystem items working together at the equipment/subsystem level to perform the specified function.

The "Equipment/Subsystem Level" identifies the major equipment, subsystems, and components currently being developed by the Repository Subsurface Design Group to perform the functions identified on the primary function level above. The primary function level above contains the design requirements, while the equipment/subsystem level identifies design solutions.

The "Operation Level" identifies the basic operational functions that each piece of equipment or subsystem is to accomplish. Each equipment/subsystem level item can be described by the group of operations it performs. These various operations may occur either simultaneously, sequentially, or in some combination of the two. The operational items are generally realized through the components at the monitoring/control level that have been designed to carry them out.

The "Monitoring/Control Level" identifies the specific functional descriptions of primary process monitoring or control activities. The items identified on this level are functionally responsible for executing the operations identified on the operation level above through the workings of the physical process or communication devices identified on the device level below.

The "Device Level" identifies discrete and analog I&C-related or communication components that physically carry out the functional activities identified at the monitoring/control level. Device level interfaces will primarily be by means of analog and digital electronic signals, but may also include pneumatic signals as well. These elements serve primarily as inputs or outputs to the monitoring/control level functions. As individual inputs to a process, they supply information to SSCs located on the monitoring/control level. As process conditions change, the state of the information sensed by these devices undergoes a change and these devices, in turn, report the change to the monitoring/control system for the process. As individual output devices, they receive information from the SSCs located on the monitoring/control level. As control functions change (usually in response to changes in process conditions), the physical state of these devices undergoes a change. In other words, the control system for the process effects the changes to these devices. The names given to each device on this level, along with the context of its functional hierarchy, are generally sufficient to determine whether it is an input or an output device.

### 6.2.2 Control System Functional Block Diagrams

This section describes a series of block diagrams that collectively present a preliminary functional architecture for the Subsurface Repository Integrated Control System based upon functions specified in SDDs related to the subsurface of the MGR. At the present time, all of these SDDs fall into one of the following status categories: (1) summary only, (2) draft form, (3) approved, (4) baselined. The following table summarizes the current status and QA classification levels of all SDDs represented in the functional architecture for the Subsurface Repository Integrated Control System.

Table 1. SDD Status and System QA Classification

| SDD | Reference | QA Level | Status | | | |
|---|---|---|---|---|---|---|
| | | | Summary | Drafted | Approved | Baselined |
| MGR Operations Monitoring and Control System (SU57) | DIRS 3 | QL-2 | | X | | |
| Waste Emplacement System (SS17) | DIRS 2 | QL-1 | | | | X |
| Waste Retrieval System (SS21) | DIRS 6 | QL-1 | | | | X |
| Subsurface Ventilation System (SS05) | DIRS 1 | CQ | | | | X |
| Backfill Emplacement System (SS18) | DIRS 7 | QL-2 | | | | X |
| Performance Confirmation Emplacement Drift Monitoring System (SS14) | DIRS 5 | QL-3 | | | | X |
| Ground Control System (SS03) | DIRS 4 | QL-2 | | | | X |
| Subsurface Electrical Distribution System (SS06) | DIRS 10 | CQ | | | X | |
| Subsurface Excavation System (SS25) | DIRS 11 | CQ | | | X | |
| Subsurface Fire Protection (SS26) | DIRS 9 | CQ | | | X | |
| Performance Confirmation Data Acquisition/Monitoring System (SU55) | DIRS 8 | QL-3 | | | X | |
| Subsurface Emplacement Transportation System (SS24) | N/A | CQ | X | | | |
| Subsurface Development Transportation System (SS16) | N/A | CQ | X | | | |
| Subsurface Compressed Air System (SS08) | N/A | CQ | X | | | |
| Subsurface Water Collection/Removal System (SS20) | N/A | CQ | X | | | |
| Subsurface Water Distribution System (SS09) | N/A | CQ | X | | | |
| Muck Handling System (SS15) | N/A | CQ | X | | | |

#### 6.2.2.1 MGR Operations Monitoring and Control System

The MGR is composed of the Waste Handling System (WHS), the Waste Isolation System (WIS), and the Operational Support System (OSS). A key system supporting the OSS is the MGR OMCS. The hierarchical structure of these systems is described and shown in the *Monitored Geologic Repository Architecture* document (DIRS 27).

The control system functional block diagram for the subsurface portion of the MGR OMCS, known as the Subsurface Repository Integrated Control System, appears in Figure 1. As indicated in this figure, the Subsurface Repository Integrated Control System is the focal point for all key subsurface monitoring, control, and communication functions. In fact, virtually all subsurface-related process systems (safety as well as non-safety) will be remotely monitored and/or controlled from the OMCS facility. Among these systems are those represented by SDDs that appear on the system level of the figure. Other process systems and all subsurface communications systems are shown at the equipment/subsystem level.

A number of human-machine interface (HMI) workstation computers identified on the device level in Figure 1 will provide real-time feedback to operations personnel, giving them a global perspective on the overall operational status and performance of various subsurface process systems. These workstations will provide operators with the capability to control and/or shutdown key processes under both normal and off-normal conditions. These same workstations will also allow operators to initiate a recovery sequence or a re-start of these same systems. Also shown on the device level are operator input and data output devices. These are the control switches that would typically accompany the workstation computers to enable operations personnel to perform their monitoring and control activities. Operator input devices are items such as keyboards and mouse controls, while data output devices generally include video monitors and printers. The device level also includes data storage devices, which are computer workstation and network server components such as disk and tape drives used for application program storage and data archiving. Finally, the group of components located on the device level termed process monitoring and control devices are the distributed control systems (DCSs), programmable logic controllers (PLCs), and specialty monitoring panels and process controllers located throughout the subsurface facility. It is through these components that primary process monitoring and control takes place.

The MGR OMCS comprises both surface and subsurface monitoring and control operations. These two integrated control systems will likely need to share status and control parameters for dispatched rail traffic movement between surface and subsurface locations during emplacement, retrieval, construction development activities, and backfilling operations. Also shown in the figure are several site-level systems that the Subsurface Repository Integrated Control System (the subsurface portion of the MGR OMCS) interfaces with. The Subsurface Repository Integrated Control System interfaces with the Site Communications System via a site-wide local area network for archival storage of operational data, and on-site and off-site digital communications. The Site Communications System will also provide the Subsurface Repository Integrated Control System with on-site and off-site voice communication via a private automatic branch exchange telephone system link, a site-wide public address system, and a site-wide radio system. The Subsurface Repository Integrated Control System interfaces with the Safeguards and Security System to provide system operational status and emergency alarm indications. The

Subsurface Repository Integrated Control System interfaces with the Site Operation System to provide site-wide acquisition of data for analyses and reports, historical information for trends, and utility information for plant operation. The Site Operation System will also provide the Subsurface Repository Integrated Control System with operating plans and procedures. These interfaces are described in the summary section of the *Monitored Geologic Repository Operations Monitoring and Control System Description Document* (DIRS 3).

#### 6.2.2.2 Waste Emplacement System

Figures 2 through 4 show control system functional block diagrams for the Waste Emplacement System (DIRS 2). The Waste Emplacement System has been the focus of several other design documents and, as developed in the figures, represents a higher level of design detail than that shown for some of the other systems (see DIRS 19, DIRS 22, DIRS 23, and DIRS 24). The operational capabilities and parameters of the transport locomotives, waste package transporters, emplacement gantries, and emplacement gantry carriers are described in the references cited.

As shown at the operation level of Figures 2 through 4, the onboard radiological monitoring system for the locomotives, transporters, and gantries interfaces with that portion of the subsurface radiological monitoring system (Figure 13) responsible for the radiological monitoring of mobile vehicles. Also shown on the same level, the onboard fire detection system for these same vehicles interfaces with that portion of the Subsurface Fire Protection System (Figure 14) responsible for detecting mobile vehicle fires. As shown in Figure 11, the temperature and air quality controls for the subsurface emplacement area ventilation system provide interlocks for the door controls. Also interlocked at this level, as shown in the figures, are the brake and alignment controls for the waste package transporter and emplacement gantry carrier coupled to a transport locomotive. Thus, when the locomotive brakes are applied, the brakes of the emplacement vehicles coupled to it are also applied. The brakes of the waste retrieval covered shuttle car, waste retrieval utility rail car, and backfill shuttle car, are also each interlocked with the brakes of the locomotive transporting them (Figures 9 and 10). The locomotive brakes are interlocked with its own drive controls so that the locomotive will not continue throttling once its brakes are applied. As shown in Figure 5, the locomotive brakes and drive controls are also interlocked with the collision avoidance system for subsurface rail traffic, which automatically maintains a safe stopping distance between it and other rail traffic that may be present on the same section of track.

#### 6.2.2.3 Subsurface Emplacement Transportation System

Figure 5 depicts the control system functional block diagram for the Subsurface Waste Transportation System. The functions associated with this system have not been finalized and are subject to change or revision (see Assumptions 5.1, 5.2 and 5.3). Equipment, instrumentation, signaling, operational sequences and parameters, and alarm features pertaining to the overhead trolley and third rail power systems are described in DIRS 25.

As shown at the control/monitoring level of Figure 5, the system that monitors the location of each train underground is interlocked with the speed controls for all trains. A train's speed controls for collision avoidance are, in turn, interlocked with the throttle and brake controls of its locomotive as shown in Figure 3. These interfaces ensure that minimum safe distances are maintained at all times between all trains throughout the subsurface to prevent collisions.

#### 6.2.2.4 Performance Confirmation Emplacement Drift Monitoring System

The control system functional block diagram for the Performance Confirmation Emplacement Drift Monitoring System (DIRS 5) is shown in Figure 6. This system has been the focus of other design documents (DIRS 21) and, therefore, some design detail is available. The operational sequence and control system details pertaining to the remote inspection gantry components are described in the *Performance Confirmation Data Acquisition System* (DIRS 21).

#### 6.2.2.5 Performance Confirmation Data Acquisition/Monitoring System

Figure 7 depicts the control system block diagram for the Subsurface Performance Confirmation Data Acquisition and Monitoring System (DIRS 8). This system is currently categorized as a surface-related SDD. However, as indicated in the figure, a significant majority of the operations associated with this system are performed throughout the subsurface repository. Previously, the functions associated with this system were combined into a single subsurface system covering the entire performance confirmation program. Additional design information can be obtained from the *Performance Confirmation Data Acquisition System* design document (DIRS 21).

The monitoring/control level in Figure 7 identifies several monitoring interfaces between the Performance Confirmation Data Acquisition/Monitoring System and the subsurface ventilation system for emplacement areas. These performance confirmation monitoring operations utilize data gathered from the various air temperature, relative humidity, radioactive particulate, and radon gas monitoring devices as shown in Figure 11. The Performance Confirmation Data Acquisition/Monitoring System also collects emplaced waste package data via a remotely operated inspection gantry. A functional diagram of this gantry is given in Figure 6.

#### 6.2.2.6 Waste Retrieval System

The control system functional block diagram for the Waste Retrieval System (DIRS 6) is shown in Figures 8 and 9. The equipment for normal waste package retrieval will be the same as that for waste package emplacement. Furthermore, control system operations for normal waste package retrieval are essentially the same as those for waste package emplacement, except in reverse sequential order. As such, the operations associated with normal waste package retrieval are interfaced at the equipment/subsystem level with waste package emplacement equipment as shown in Figures 3 through 4. In Figure 9, the utility rail and covered shuttle car brakes are interlocked at the monitoring/control level with the brake controls of the locomotive transporting them. Preliminary control system design concepts for off-normal retrieval scenarios are briefly outlined in another design document (DIRS 33).

#### 6.2.2.7 Backfill Emplacement System

Figure 10 depicts the control system functional block diagram for the Backfill Emplacement System (DIRS 7). Equipment, instrumentation, and control system details pertaining to the transportation and placement of backfill material within the emplacement drifts are still in the development stages.

The operations associated with the transportation of loaded backfill material aboard shuttle cars to the subsurface areas are interfaced at the equipment/subsystem level with transport locomotives used for waste package emplacement/retrieval as shown in Figure 3. The shuttle car brakes are interlocked at the monitoring/control level with the brake controls of the locomotive transporting it. Mobile conveyors are then used to transport the backfill material from the shuttle cars to the emplacement drifts. These operations are briefly described in Section 5.3.1 of the *Viability Assessment of a Repository at Yucca Mountain – Preliminary Design Concept for the Repository and Waste Package, Volume 2* (DIRS 32).

### 6.2.2.8 Subsurface Ventilation System

The control system functional block diagram for the Subsurface Ventilation System (DIRS 1) is shown in Figures 11 and 12. For protection from possible radionuclide contamination, the ventilation system is divided into two separate and isolated systems, one covering only the construction development area (see Figure 12), and one covering only the emplacement area (see Figure 11). The design details of the ventilation control system, as well as determination of the quantities and operational sequences of the fans, valves, and dampers for the subsurface air delivery system, are still in the process of development. An overview description of the Subsurface Ventilation System is presented in Section 4.2.4 of the *Viability Assessment of a Repository at Yucca Mountain – Preliminary Design Concept for the Repository and Waste Package, Volume 2* (DIRS 32).

As shown at the equipment/subsystem level of Figure 11, human access to the emplacement drifts is controlled through operation of the drift isolation doors depicted in Figure 2. The door controls are also interlocked at the monitoring/control level of the emplacement area ventilation system, with the temperature, air quality, and isolation valve controls as shown in Figure 11, since these ventilation system parameters are directly affected by the various combinations of door positions. The emplacement area ventilation system interfaces with the Subsurface Fire Protection System (Figure 14) at the monitoring/control level of Figure 11 by incorporating data from smoke and combustible gas detectors as part of the emplacement ventilation system air quality controls. The emplacement area ventilation system also maintains a reporting interface with the subsurface air monitoring system (see Figure 13) at the monitoring/control level of Figure 11 by providing the subsurface air monitoring system with subsurface air quality data. Control system interlocks at the monitoring/control level within the emplacement area ventilation system include the actuator and drive controls for the various air flow valves, isolation valves, regulating dampers, booster fans, and exhaust fans as part of the temperature and air quality control systems. Clearly, these interlocks are necessary to allow regulation of air temperatures and to maintain air quality throughout the subsurface facility during waste emplacement operations. Finally, the emplacement area ventilation system interfaces with the Performance Confirmation Data Acquisition and Monitoring System (Figure 7) at the monitoring/control level of Figure 11 by supplying the performance confirmation system with data gathered from the various air temperature, relative humidity, radioactive particulate, and radon gas monitoring devices as shown in Figure 11.

Like the emplacement area ventilation system, the development area ventilation system shown in Figure 12 interfaces with the Subsurface Fire Protection System (Figure 14) at the monitoring/control level by incorporating data from smoke and combustible gas detectors as part of the development ventilation system air quality controls. Also depicted at this point is a reporting interface with the subsurface air monitoring system (see Figure 13), which provides the subsurface air monitoring system with subsurface air quality data. Furthermore, control system interlocks at this same level within the development area ventilation system include the actuator and drive controls for the various air flow valves, regulating dampers, construction fans, and booster fans as part of the temperature and air quality control systems. These interlocks are essential for regulating air temperatures and maintaining air quality throughout the subsurface facility during its construction stages.

As shown on the monitoring/control level of Figures 11 and 12, a reporting interface is maintained between the emplacement area ventilation system and the development area ventilation system. This interface is provided just in case it becomes necessary for one system to monitor the air quality control parameters of the other system during upset conditions or in an emergency situation.

### 6.2.2.9 Subsurface Radiological and Air Monitoring Systems

Figure 13 depicts the control system functional block diagram for the radiological and air monitoring systems throughout the subsurface facility. As shown in the figure, air quality data are provided to the air monitoring system at the control/monitoring level from the air quality controls for both the emplacement area and development area ventilation systems (Figures 11 and 12). Shown at the operation level of Figure 13 are reporting interfaces to the radiological monitoring system from the mobile vehicles used for waste emplacement and retrieval operations (Figures 2 through 4).

### 6.2.2.10 Subsurface Fire Protection System

Figure 14 depicts the control system functional block diagram for the Subsurface Fire Suppression System (DIRS 9). Equipment requirements, instrumentation, operational sequences, and control system details pertaining to the subsurface vehicle and facility fire protection subsystems are still in the process of development. The functions associated with this system have not been finalized and are subject to change or revision.

Appearing at the operation level of Figure 14 are reporting interfaces to the Subsurface Fire Detection and Notification System from the mobile vehicles used for waste emplacement and retrieval operations (Figures 2 through 4). The monitoring/control level of the figure shows reporting interfaces to the emplacement and development ventilation systems (Figures 11 and 12) from the smoke and combustible gas detectors used for fire detection. The combustible gas detectors are interlocked with the circuit breaker trip controls for the Subsurface Electrical Distribution System (Figure 16) at the monitoring/control level of Figure 14. The purpose of this interlock is to shut off electrical power in areas where an explosive atmosphere is detected so that electrical arcing is eliminated as a possible ignition source.

#### 6.2.2.11 Subsurface Communications

Figure 15 depicts the control system functional block diagram for subsurface voice, video, and data communications. Quantities, distribution and arrangement, and control system details pertaining to voice and video communications equipment throughout the subsurface are still in the process of development. However, a preliminary design concept for subsurface facility-wide voice and video communications networks is presented in Section 6.3 of this document. Other analyses and reports have evaluated various concepts for portions of the subsurface data communications network (DIRS 19 and DIRS 24) and a preliminary design concept for a data communication system integrating the entire subsurface repository is presented Section 6.4 of this document.

Appearing at the equipment/subsystem level is a voice communications link between the site Private Automatic Branch Exchange telephone system and the subsurface page/party communications system. This interface gives both local and long distance calling capability to the subsurface page/party system handsets, thus eliminating the need for an additional distribution network of telephone handsets throughout the subsurface facility. There is also another voice communications link at the equipment/subsystem level between the site public address system and the subsurface page/party system. This interface allows the public address system to utilize the page/party system's network of amplifiers and loudspeakers.

#### 6.2.2.12 Subsurface Electrical Distribution System

Figure 16 depicts the control system functional block diagram for the Subsurface Electrical Distribution System (DIRS 10). The functions associated with this system have not been finalized and are subject to change or revision. Quantities and arrangements pertaining to electrical power distribution equipment located throughout the subsurface facility are described in DIRS 26.

As shown at the monitoring/control level of Figure 16, area combustible gas detectors for the Subsurface Explosive Hazard Detection System (Figure 14) are interlocked with trip controls for circuit breakers delivering power throughout the subsurface facility. The purpose of this interlock is to shut off electrical power in areas where an explosive atmosphere is detected so that electrical arcing is eliminated as a possible ignition source.

#### 6.2.2.13 Subsurface Utilities

Preliminary control system functional block diagrams of subsurface compressed air, water distribution, and water collection/removal systems are depicted in Figure 17. Equipment requirements, operational sequences, and control system details pertaining to these subsurface utilities are still in the process of development (see Assumptions 5.4, 5.5, 5.6, 5.7, and 5.8). The functions associated with these systems have not been finalized and are subject to change or revision.

As shown in Figure 17 for the monitoring/control level of the Water Collection/Removal System, the level monitoring system for the water collection sumps is interlocked with the sump pump controls for water removal. Specifically, a high sump level will automatically start its associated water removal pump. Shown at the equipment/subsystem level of the figure is a surface-based treatment system for the water that collects in these sumps and is pumped out. The required equipment and operational features of this system have not yet been considered.

#### 6.2.2.14 Subsurface Construction Development Systems

Figure 18 depicts a preliminary control system functional block diagram for the Subsurface Excavation System (DIRS 11), the Muck Handling System, and the Subsurface Development Transportation System. An overview of the major equipment items pertaining to these systems is presented in DIRS 30.

Equipment requirements, operational strategies and sequences, and control system details pertaining to these systems are still in the process of development (see Assumptions 5.9 and 5.10). The functions associated with these systems have not been finalized and are subject to change or revision.

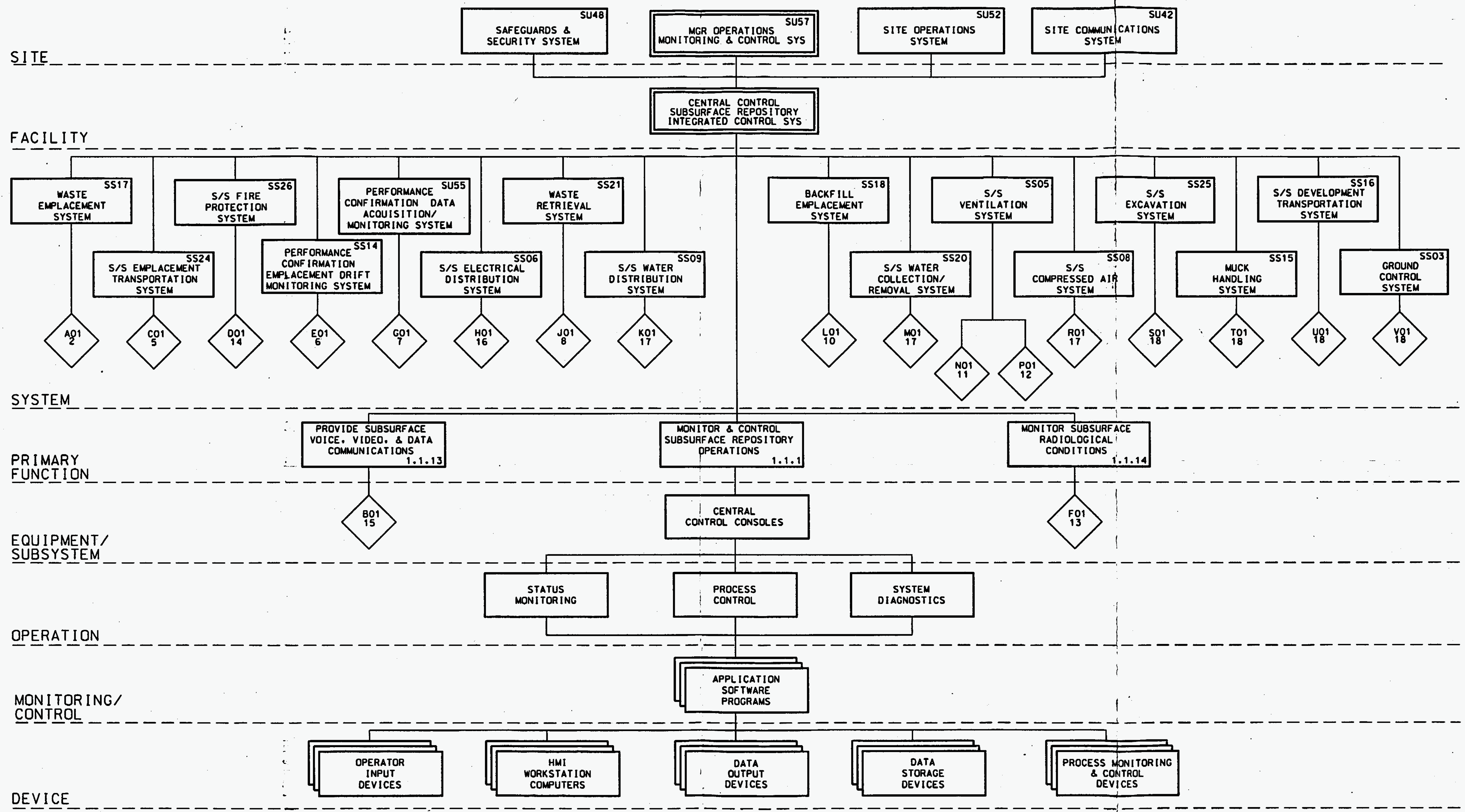
The functional diagram for the Ground Control System (DIRS 4), is shown in Figure 18. Primarily a measurement and sensing system, the Ground Control System will utilize specialized geophysical instrumentation to detect potential stress buildup in the rock mass throughout the subsurface. The quantities and types of geophysical pressure instrumentation are still in the process of development. See also Section 7.7.1 of DIRS 21 for some types of in-situ devices that are likely to be used throughout this system.

The functional diagram for the Subsurface Development Transportation System is shown in Figure 18. The brakes of the rail haulage car are interlocked at the monitoring/control level with the brake controls of the locomotive transporting it.

### 6.2.3 Control System Functional Block Diagram Summary

The control system functional block diagrams presented at the end of this section (Figures 1 through 18) provide a valuable basis for examining the overall size, complexity, and interfaces of the Subsurface Repository Integrated Control System.

These figures are expected to have several important uses as the design of the overall subsurface control system continues to evolve. First, the most obvious and perhaps most immediate purpose for these figures lies in their illustrative utility as companion diagrams for the SDDs from which they are derived. They graphically demonstrate the functional hierarchy, peer system interfaces, and monitoring/control interlocks for each of their respective SDDs. Secondly, these figures help ensure that SDD functions are appropriately mapped onto physical process components. Insofar as these diagrams identify the functions of SSCs associated with a given process system, they will supply the necessary information for developing more detailed equipment and instrumentation lists as the design effort progresses. Thirdly, given that they show the various peer system interfaces for each SDD system, they will assist in determining primary control interfaces and interlocks between subsurface systems that are functionally separated from one another. Finally, as hierarchical diagrams depicting the functional interconnections within a given system, they will provide an important resource for developing I&C process and instrumentation diagrams and the Boolean structure of control system logic diagrams. This information, in turn, will assist in generating detailed input and output lists for the Subsurface Repository Integrated Control System design.


SITE
FACILITY
SYSTEM
PRIMARY FUNCTION
EQUIPMENT/ SUBSYSTEM
OPERATION
MONITORING/ CONTROL
DEVICE
SU48 SAFEGUARDS & SECURITY SYSTEM
SU57 MGR OPERATIONS MONITORING & CONTROL SYS
SU52 SITE OPERATIONS SYSTEM
SU42 SITE COMMUNICATIONS SYSTEM
CENTRAL CONTROL SUBSURFACE REPOSITORY INTEGRATED CONTROL SYS
SS17 WASTE EMPLACEMENT SYSTEM
SS24 S/S EMPLACEMENT TRANSPORTATION SYSTEM
SS26 S/S FIRE PROTECTION SYSTEM
SS14 PERFORMANCE CONFIRMATION EMPLACEMENT DRIFT MONITORING SYSTEM
SS55 PERFORMANCE CONFIRMATION DATA ACQUISITION/ MONITORING SYSTEM
SS06 S/S ELECTRICAL DISTRIBUTION SYSTEM
SS21 WASTE RETRIEVAL SYSTEM
SS09 S/S WATER DISTRIBUTION SYSTEM
SS18 BACKFILL EMPLACEMENT SYSTEM
SS20 S/S WATER COLLECTION/ REMOVAL SYSTEM
SS05 S/S VENTILATION SYSTEM
SS08 S/S COMPRESSED AIR SYSTEM
SS25 S/S EXCAVATION SYSTEM
SS15 MUCK HANDLING SYSTEM
SS16 S/S DEVELOPMENT TRANSPORTATION SYSTEM
SS03 GROUND CONTROL SYSTEM
A01 2
C01 5
D01 14
E01 6
G01 7
H01 16
J01 8
K01 17
L01 10
M01 17
N01 11
P01 12
R01 17
S01 18
T01 18
U01 18
V01 18
PROVIDE SUBSURFACE VOICE, VIDEO, & DATA COMMUNICATIONS 1.1.13
MONITOR & CONTROL SUBSURFACE REPOSITORY OPERATIONS 1.1.1
MONITOR SUBSURFACE RADIOLOGICAL CONDITIONS 1.1.14
B01 15
F01 13
CENTRAL CONTROL CONSOLES
STATUS MONITORING
PROCESS CONTROL
SYSTEM DIAGNOSTICS
APPLICATION SOFTWARE PROGRAMS
OPERATOR INPUT DEVICES
HMI WORKSTATION COMPUTERS
DATA OUTPUT DEVICES
DATA STORAGE DEVICES
PROCESS MONITORING & CONTROL DEVICES

LEGEND:

INTERCONNECTION POINT TO SYSTEMS ON OTHER FIGURES

XXX X —CONTINUATION IDENTIFIER NO.
—FIGURE NO.

NOTES:

1. DOUBLE BOXES INDICATE PRIMARY SYSTEM DEPICTED IN THIS FIGURE.

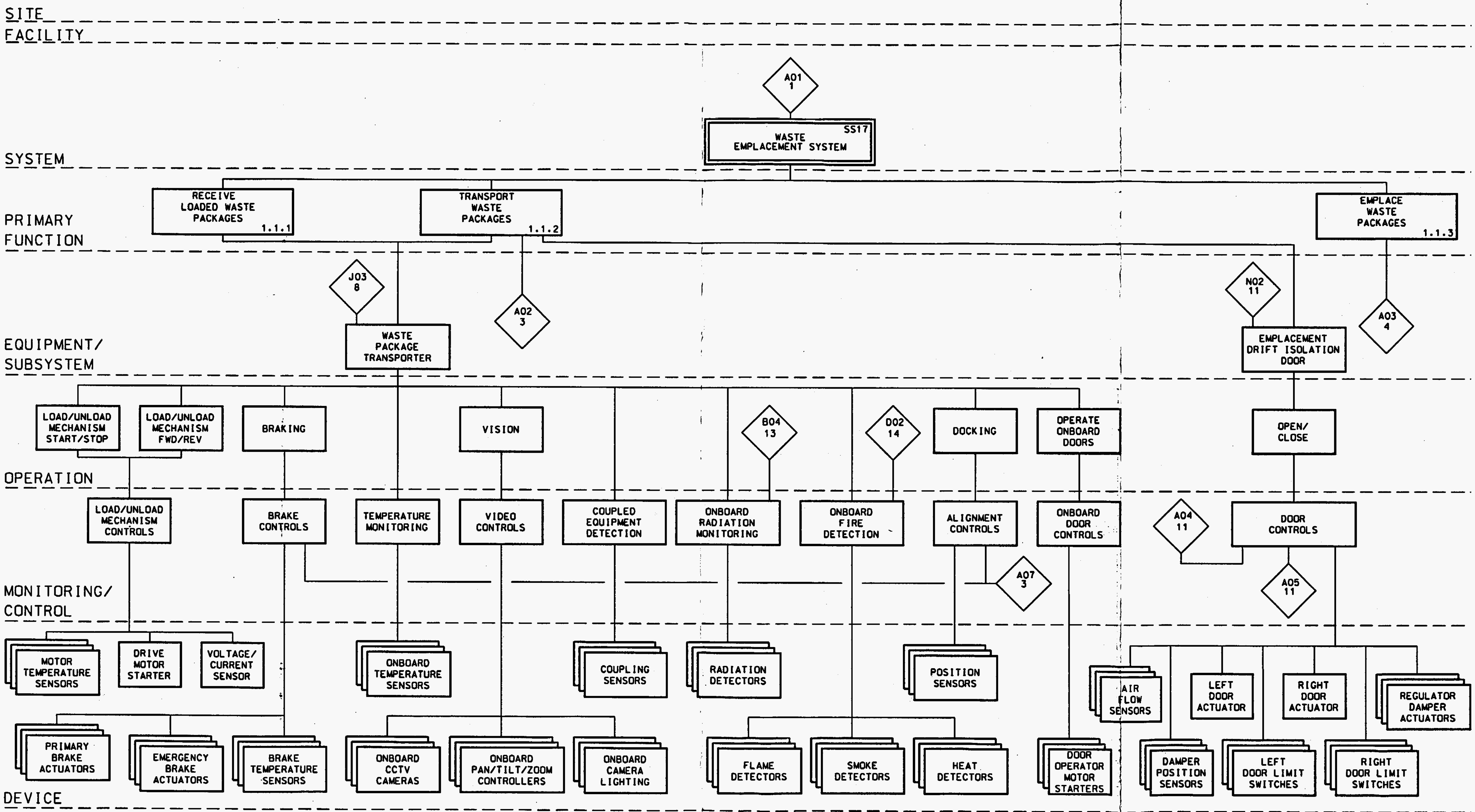
2. STACKED BOXES INDICATE MULTIPLE DEVICES/SYSTEMS

3. S/S - SUBSURFACE

t:*repss*csys*fig*sscs0046.fig

FIGURE 1
FUNCTIONAL BLOCK DIAGRAM
SUBSURFACE REP INT CONTROL SYS

FILE NAME: W03969/CSYS/FIG/SSCS0046.FIG PD: 09/24/99



LEGEND:

INTERCONNECTION POINT TO SYSTEMS ON OTHER FIGURES

◇ XXX — CONTINUATION IDENTIFIER NO.
   X — FIGURE NO.

NOTES:

1. DOUBLE BOXES INDICATE PRIMARY SYSTEM DEPICTED IN THIS FIGURE.

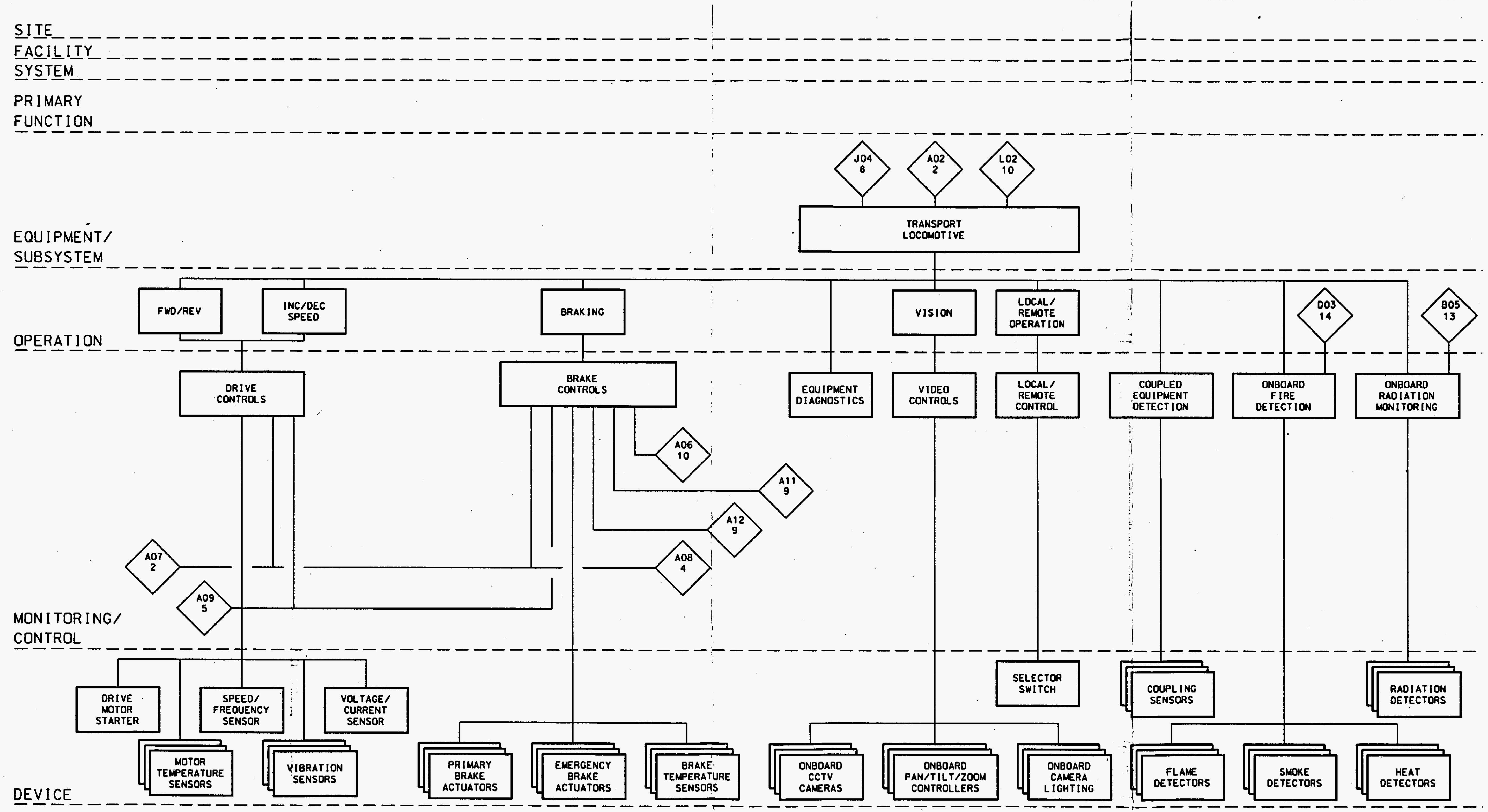
2. STACKED BOXES INDICATE MULTIPLE DEVICES/SYSTEMS

3. S/S - SUBSURFACE

t:#repss#csys#fig#sscs0047.fig

FIGURE 2
FUNCTIONAL BLOCK DIAGRAM
WASTE EMPLACEMENT SYSTEM - SHT 1

FILE NAME: W03969/CSYS/FIG/SSCS0047.FIG PD: 09/24/99



## LEGEND:

INTERCONNECTION POINT TO
SYSTEMS ON OTHER FIGURES

XXX X —CONTINUATION IDENTIFIER NO.
—FIGURE NO.

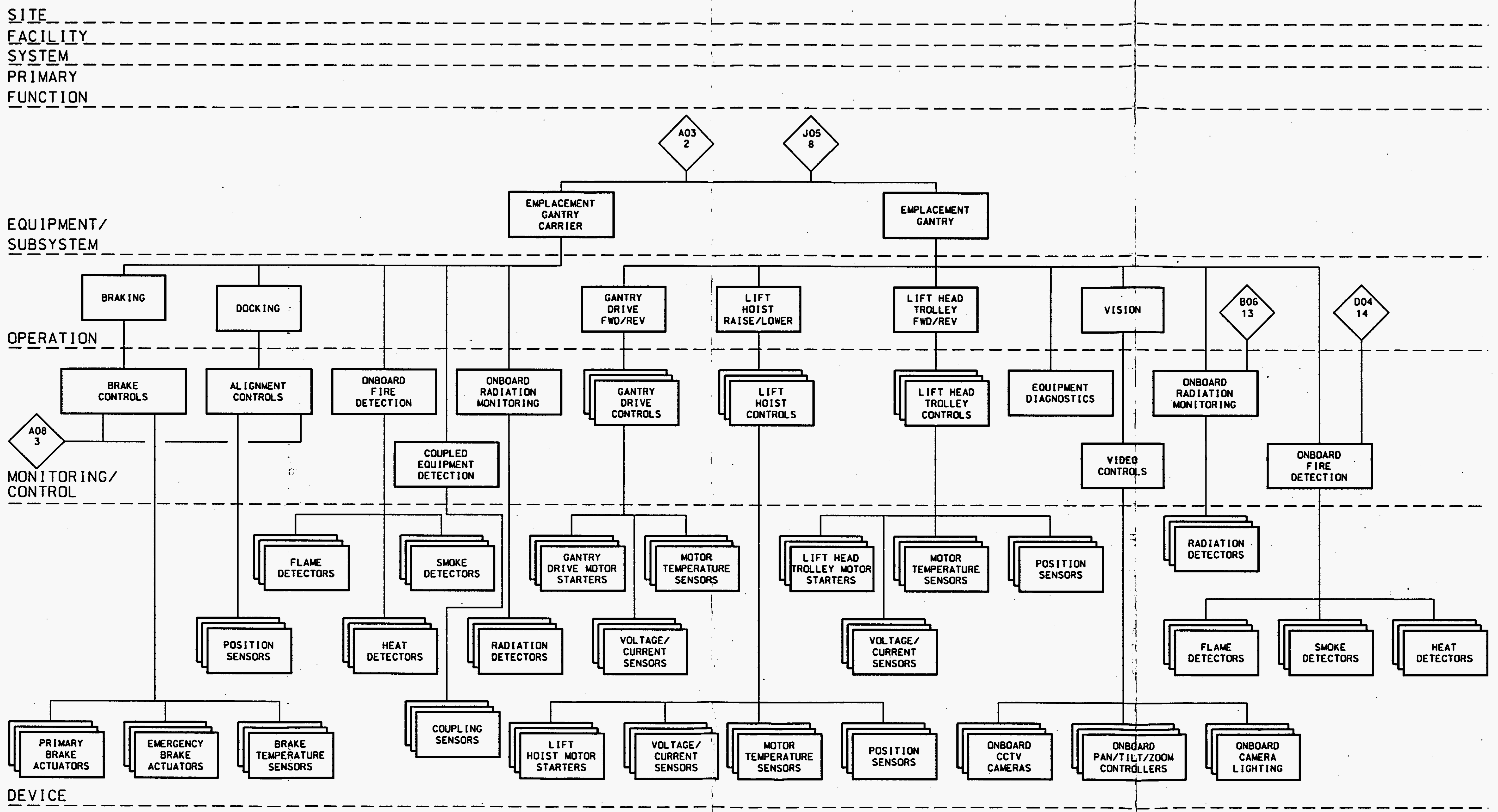
## NOTES:

1. DOUBLE BOXES INDICATE PRIMARY SYSTEM DEPICTED IN THIS FIGURE.
2. STACKED BOXES INDICATE MULTIPLE DEVICES/SYSTEMS
3. S/S - SUBSURFACE

t:*repss*csys*fig*sscs0048.fig

FIGURE 3
FUNCTIONAL BLOCK DIAGRAM
WASTE EMPLACEMENT SYSTEM - SHT 2

FILE NAME: W03969/CSYS/FIG/SSCS0048.FIG PD: 09/24/99



## LEGEND:

INTERCONNECTION POINT TO
SYSTEMS ON OTHER FIGURES

XXX —CONTINUATION IDENTIFIER NO.
X —FIGURE NO.

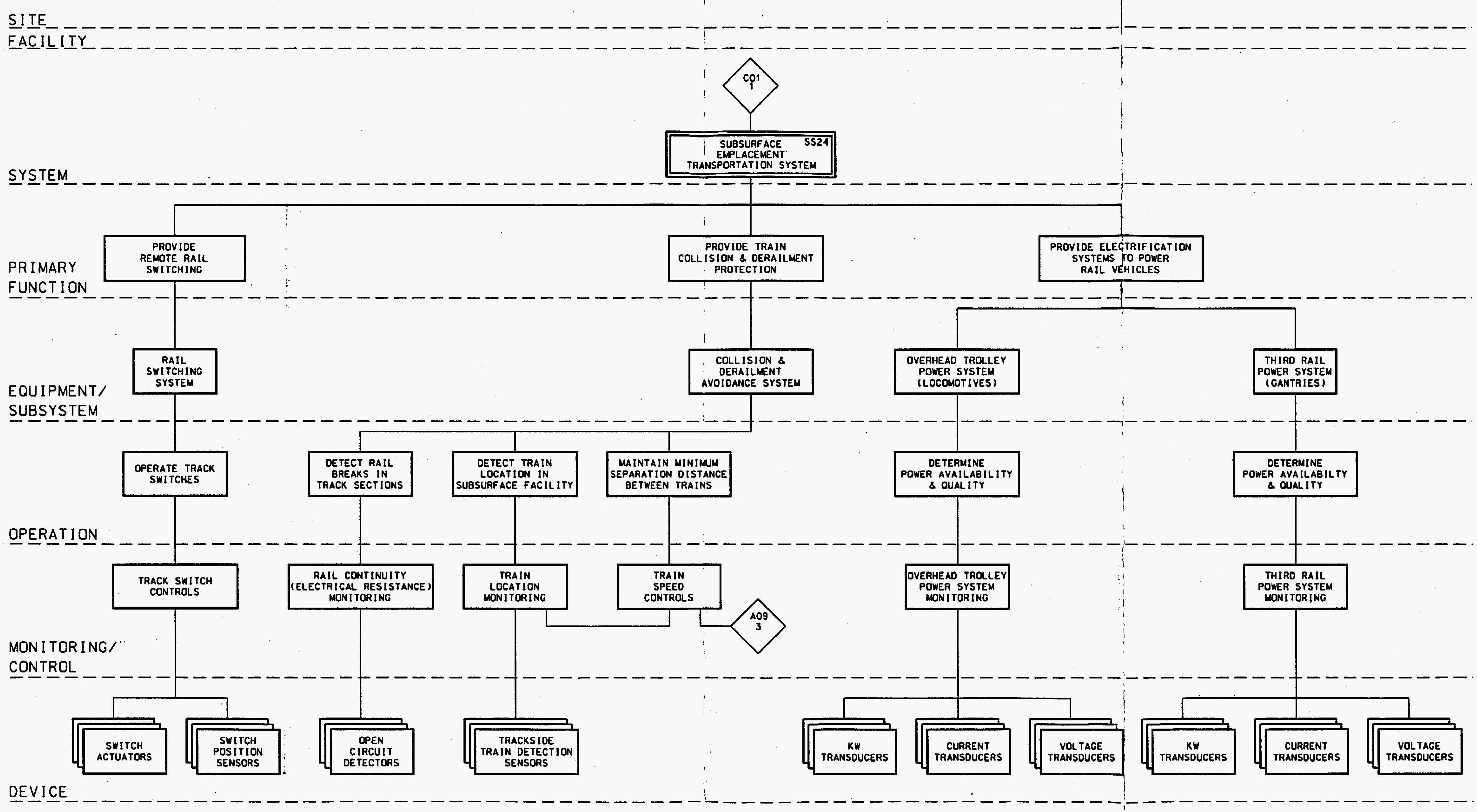
## NOTES:

1. DOUBLE BOXES INDICATE PRIMARY SYSTEM DEPICTED IN THIS FIGURE.
2. STACKED BOXES INDICATE MULTIPLE DEVICES/SYSTEMS
3. S/S – SUBSURFACE

t:*repss*csys*fig*sscs0049.fig

FIGURE 4
FUNCTIONAL BLOCK DIAGRAM
WASTE EMPLACEMENT SYSTEM – SHT 3

FILE NAME: W03969/CSYS/FIG/SSCS0049.FIG PD: 09/24/99


SITE
FACILITY
C01
1
SUBSURFACE EMPLACEMENT TRANSPORTATION SYSTEM
SS24
SYSTEM
PRIMARY FUNCTION
PROVIDE REMOTE RAIL SWITCHING
PROVIDE TRAIN COLLISION & DERAILMENT PROTECTION
PROVIDE ELECTRIFICATION SYSTEMS TO POWER RAIL VEHICLES
EQUIPMENT/ SUBSYSTEM
RAIL SWITCHING SYSTEM
COLLISION & DERAILMENT AVOIDANCE SYSTEM
OVERHEAD TROLLEY POWER SYSTEM (LOCOMOTIVES)
THIRD RAIL POWER SYSTEM (GANTRIES)
OPERATION
OPERATE TRACK SWITCHES
DETECT RAIL BREAKS IN TRACK SECTIONS
DETECT TRAIN LOCATION IN SUBSURFACE FACILITY
MAINTAIN MINIMUM SEPARATION DISTANCE BETWEEN TRAINS
DETERMINE POWER AVAILABILITY & QUALITY
DETERMINE POWER AVAILABILTY & QUALITY
MONITORING/ CONTROL
TRACK SWITCH CONTROLS
RAIL CONTINUITY (ELECTRICAL RESISTANCE) MONITORING
TRAIN LOCATION MONITORING
TRAIN SPEED CONTROLS
A09
3
OVERHEAD TROLLEY POWER SYSTEM MONITORING
THIRD RAIL POWER SYSTEM MONITORING
DEVICE
SWITCH ACTUATORS
SWITCH POSITION SENSORS
OPEN CIRCUIT DETECTORS
TRACKSIDE TRAIN DETECTION SENSORS
KW TRANSDUCERS
CURRENT TRANSDUCERS
VOLTAGE TRANSDUCERS
KW TRANSDUCERS
CURRENT TRANSDUCERS
VOLTAGE TRANSDUCERS

## LEGEND:

INTERCONNECTION POINT TO
SYSTEMS ON OTHER FIGURES

XXX
X
—CONTINUATION IDENTIFIER NO.
—FIGURE NO.

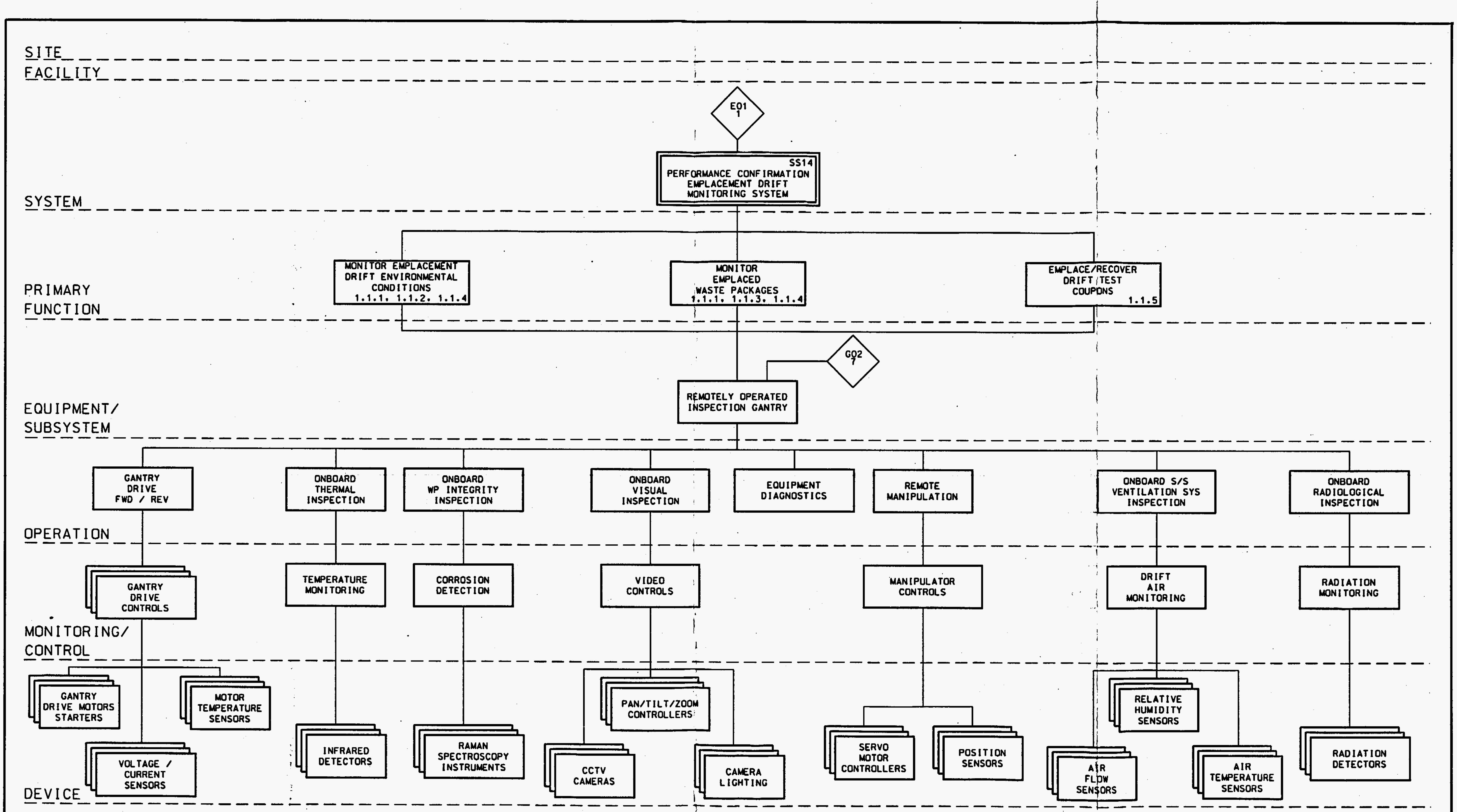
## NOTES:

1. DOUBLE BOXES INDICATE PRIMARY SYSTEM DEPICTED IN THIS FIGURE.
2. STACKED BOXES INDICATE MULTIPLE DEVICES/SYSTEMS
3. S/S - SUBSURFACE

t:*repss*csys*fig*sscs0100.fig

FIGURE 5
FUNCTIONAL BLOCK DIAGRAM
SUBSURFACE EMPLACE TRANSPORT SYS

FILE NAME: W03969/CSYS/FIG/SSCS0100.FIG PD: 09/24/99


SITE
FACILITY
E01
1
SS14
PERFORMANCE CONFIRMATION EMPLACEMENT DRIFT MONITORING SYSTEM
SYSTEM
MONITOR EMPLACEMENT DRIFT ENVIRONMENTAL CONDITIONS 1.1.1, 1.1.2, 1.1.4
MONITOR EMPLACED WASTE PACKAGES 1.1.1, 1.1.3, 1.1.4
EMPLACE/RECOVER DRIFT TEST COUPONS 1.1.5
PRIMARY FUNCTION
G02
7
REMOTELY OPERATED INSPECTION GANTRY
EQUIPMENT/ SUBSYSTEM
GANTRY DRIVE FWD / REV
ONBOARD THERMAL INSPECTION
ONBOARD WP INTEGRITY INSPECTION
ONBOARD VISUAL INSPECTION
EQUIPMENT DIAGNOSTICS
REMOTE MANIPULATION
ONBOARD S/S VENTILATION SYS INSPECTION
ONBOARD RADIOLOGICAL INSPECTION
OPERATION
GANTRY DRIVE CONTROLS
TEMPERATURE MONITORING
CORROSION DETECTION
VIDEO CONTROLS
MANIPULATOR CONTROLS
DRIFT AIR MONITORING
RADIATION MONITORING
MONITORING/ CONTROL
GANTRY DRIVE MOTORS STARTERS
MOTOR TEMPERATURE SENSORS
VOLTAGE / CURRENT SENSORS
INFRARED DETECTORS
RAMAN SPECTROSCOPY INSTRUMENTS
PAN/TILT/ZOOM CONTROLLERS
CCTV CAMERAS
CAMERA LIGHTING
SERVO MOTOR CONTROLLERS
POSITION SENSORS
RELATIVE HUMIDITY SENSORS
AIR FLOW SENSORS
AIR TEMPERATURE SENSORS
RADIATION DETECTORS
DEVICE

LEGEND:

INTERCONNECTION POINT TO
SYSTEMS ON OTHER FIGURES

XXX
X
—CONTINUATION IDENTIFIER NO.
—FIGURE NO.

NOTES:

1. DOUBLE BOXES INDICATE PRIMARY SYSTEM DEPICTED IN THIS FIGURE.

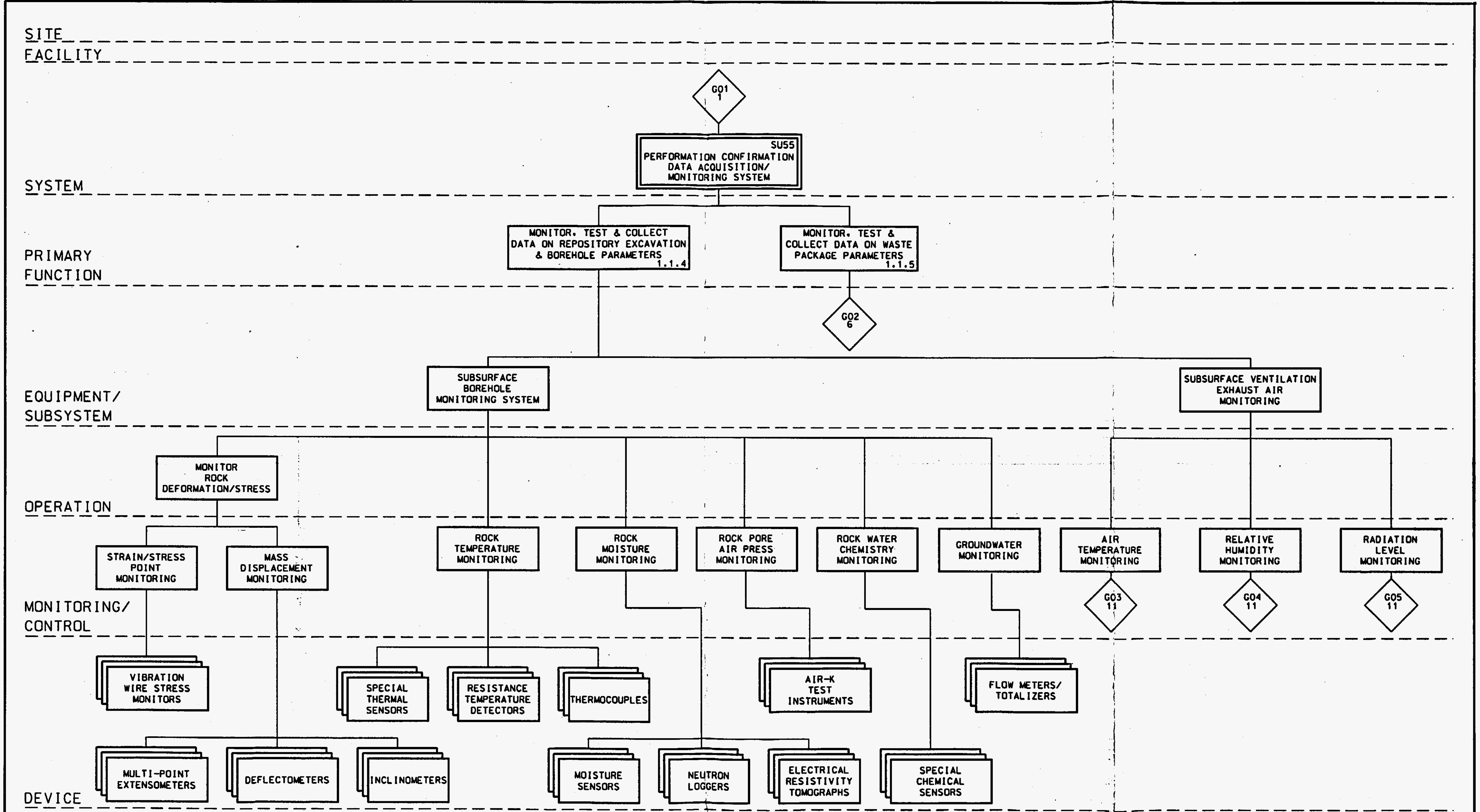
2. STACKED BOXES INDICATE MULTIPLE DEVICES/SYSTEMS

3. S/S - SUBSURFACE

t:*repss*csys*fig*sscs0101.fig

FIGURE 6
FUNCTIONAL BLOCK DIAGRAM
PC EMPLACE DRIFT MONITORING SYS

FILE NAME: W03969/CSYS/FIG/SSCS0101.FIG PD: 09/24/99


SITE
FACILITY
SYSTEM
PRIMARY FUNCTION
EQUIPMENT/ SUBSYSTEM
OPERATION
MONITORING/ CONTROL
DEVICE
G01 1
SU55 PERFORMATION CONFIRMATION DATA ACQUISITION/ MONITORING SYSTEM
MONITOR, TEST & COLLECT DATA ON REPOSITORY EXCAVATION & BOREHOLE PARAMETERS 1.1.4
MONITOR, TEST & COLLECT DATA ON WASTE PACKAGE PARAMETERS 1.1.5
G02 6
SUBSURFACE BOREHOLE MONITORING SYSTEM
SUBSURFACE VENTILATION EXHAUST AIR MONITORING
MONITOR ROCK DEFORMATION/STRESS
STRAIN/STRESS POINT MONITORING
MASS DISPLACEMENT MONITORING
ROCK TEMPERATURE MONITORING
ROCK MOISTURE MONITORING
ROCK PORE AIR PRESS MONITORING
ROCK WATER CHEMISTRY MONITORING
GROUNDWATER MONITORING
AIR TEMPERATURE MONITORING
RELATIVE HUMIDITY MONITORING
RADIATION LEVEL MONITORING
G03 11
G04 11
G05 11
VIBRATION WIRE STRESS MONITORS
SPECIAL THERMAL SENSORS
RESISTANCE TEMPERATURE DETECTORS
THERMOCOUPLES
AIR-K TEST INSTRUMENTS
FLOW METERS/ TOTALIZERS
MULTI-POINT EXTENSOMETERS
DEFLECTOMETERS
INCLINOMETERS
MOISTURE SENSORS
NEUTRON LOGGERS
ELECTRICAL RESISTIVITY TOMOGRAPHS
SPECIAL CHEMICAL SENSORS

LEGEND:

INTERCONNECTION POINT TO SYSTEMS ON OTHER FIGURES

XXX X —CONTINUATION IDENTIFIER NO.
—FIGURE NO.

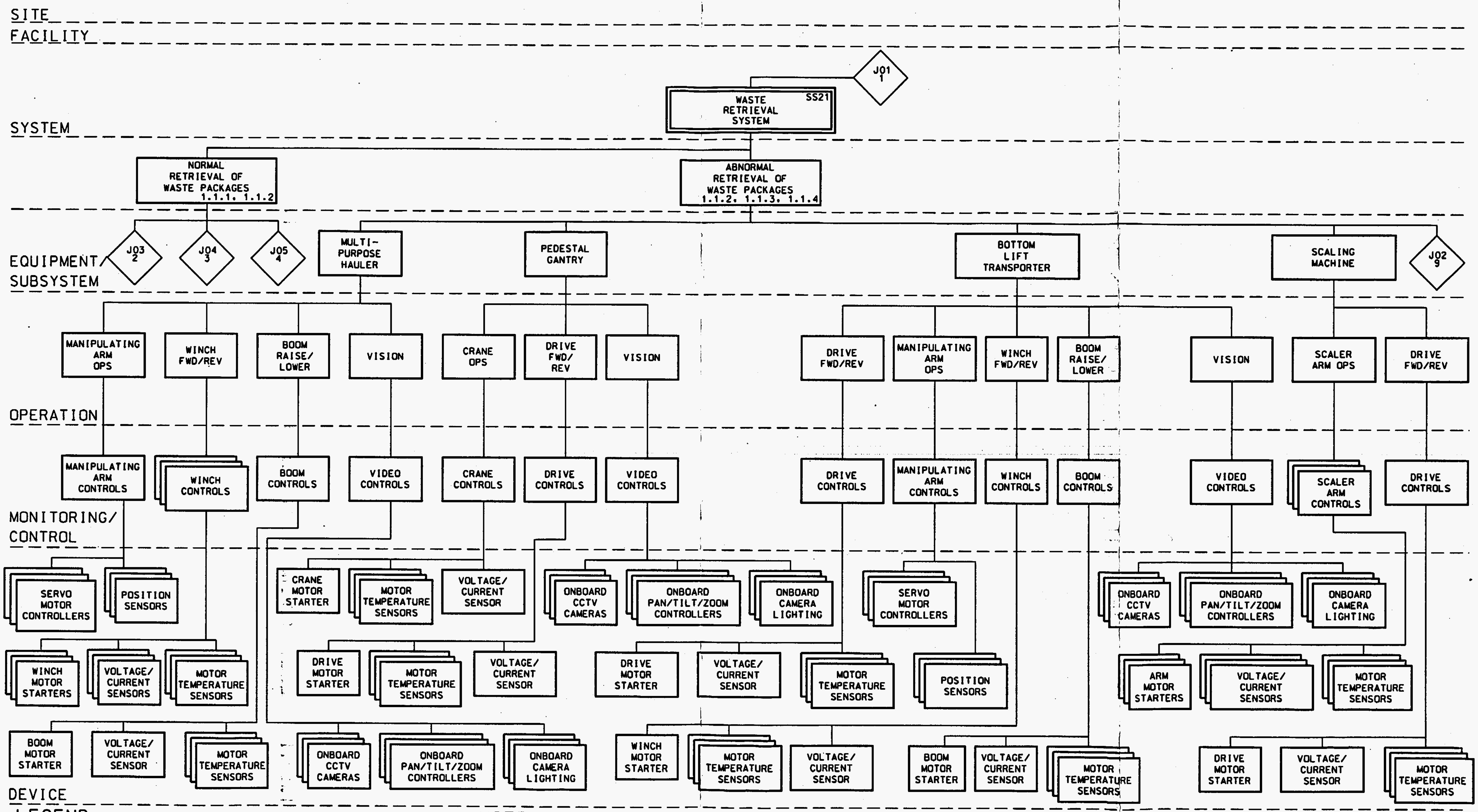
NOTES:

1. DOUBLE BOXES INDICATE PRIMARY SYSTEM DEPICTED IN THIS FIGURE.
2. STACKED BOXES INDICATE MULTIPLE DEVICES/SYSTEMS
3. S/S - SUBSURFACE

t:*repss*csys*fig*sscs0102.fig

FIGURE 7
FUNCTIONAL BLOCK DIAGRAM
PC DATA ACQUISITION/MONITOR SYS

FILE NAME: W03969/CSYS/FIG/SSCS0102.FIG PD: 09/24/99



LEGEND:

INTERCONNECTION POINT TO SYSTEMS ON OTHER FIGURES

XXX
X
CONTINUATION IDENTIFIER NO.
FIGURE NO.

NOTES:

1. DOUBLE BOXES INDICATE PRIMARY SYSTEM DEPICTED IN THIS FIGURE.

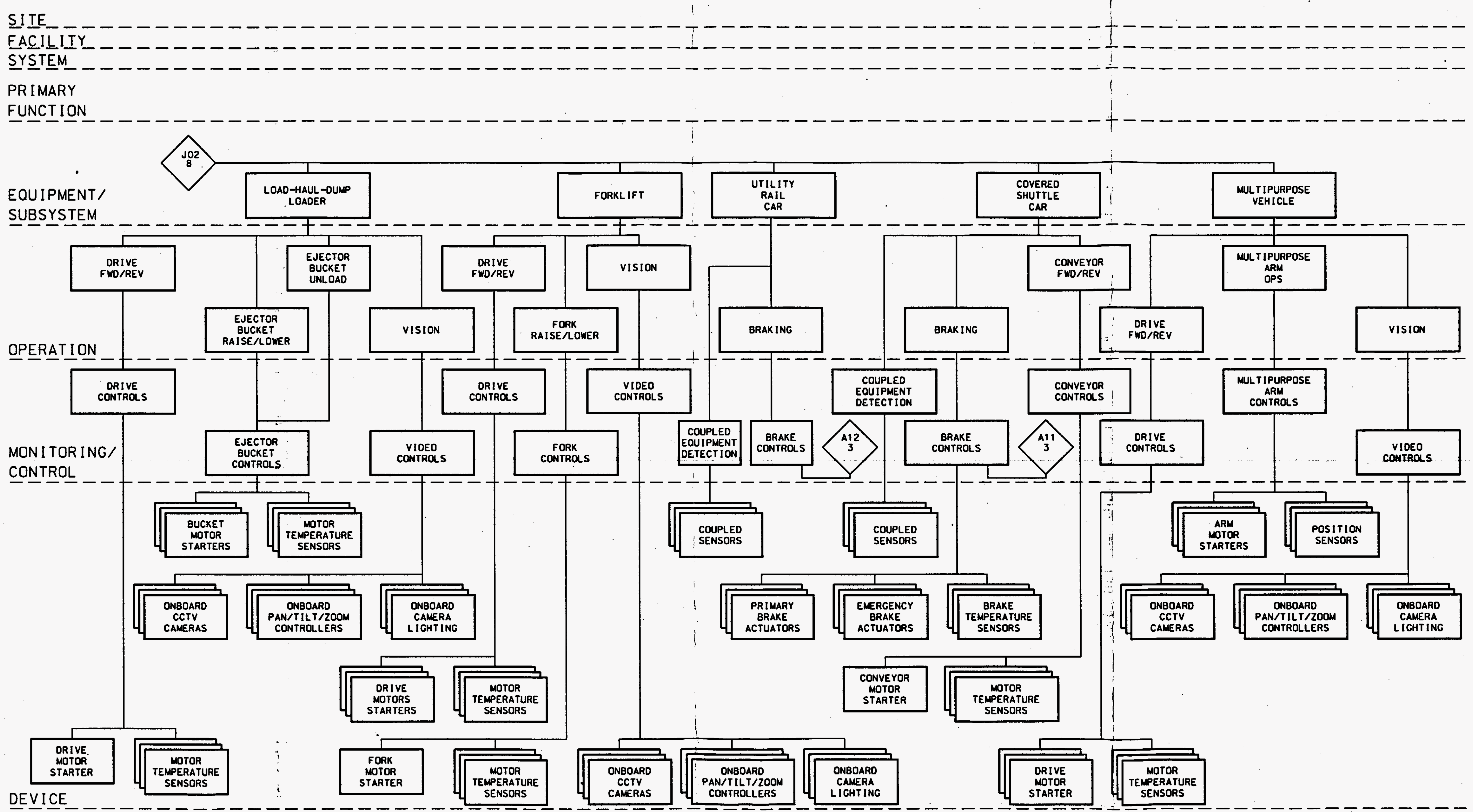
2. STACKED BOXES INDICATE MULTIPLE DEVICES/SYSTEMS

3. S/S - SUBSURFACE

t:*repss*csys*fig*sscs0103.fig

FIGURE 8
FUNCTIONAL BLOCK DIAGRAM
WASTE RETREIVAL SYSTEM - SHT 1

FILE NAME: W03969/CSYS/FIG/SSCS0103.FIG PD: 09/24/99



LEGEND:

INTERCONNECTION POINT TO
SYSTEMS ON OTHER FIGURES

XXX X —CONTINUATION IDENTIFIER NO.
—FIGURE NO.

NOTES:

1. DOUBLE BOXES INDICATE PRIMARY SYSTEM DEPICTED IN THIS FIGURE.

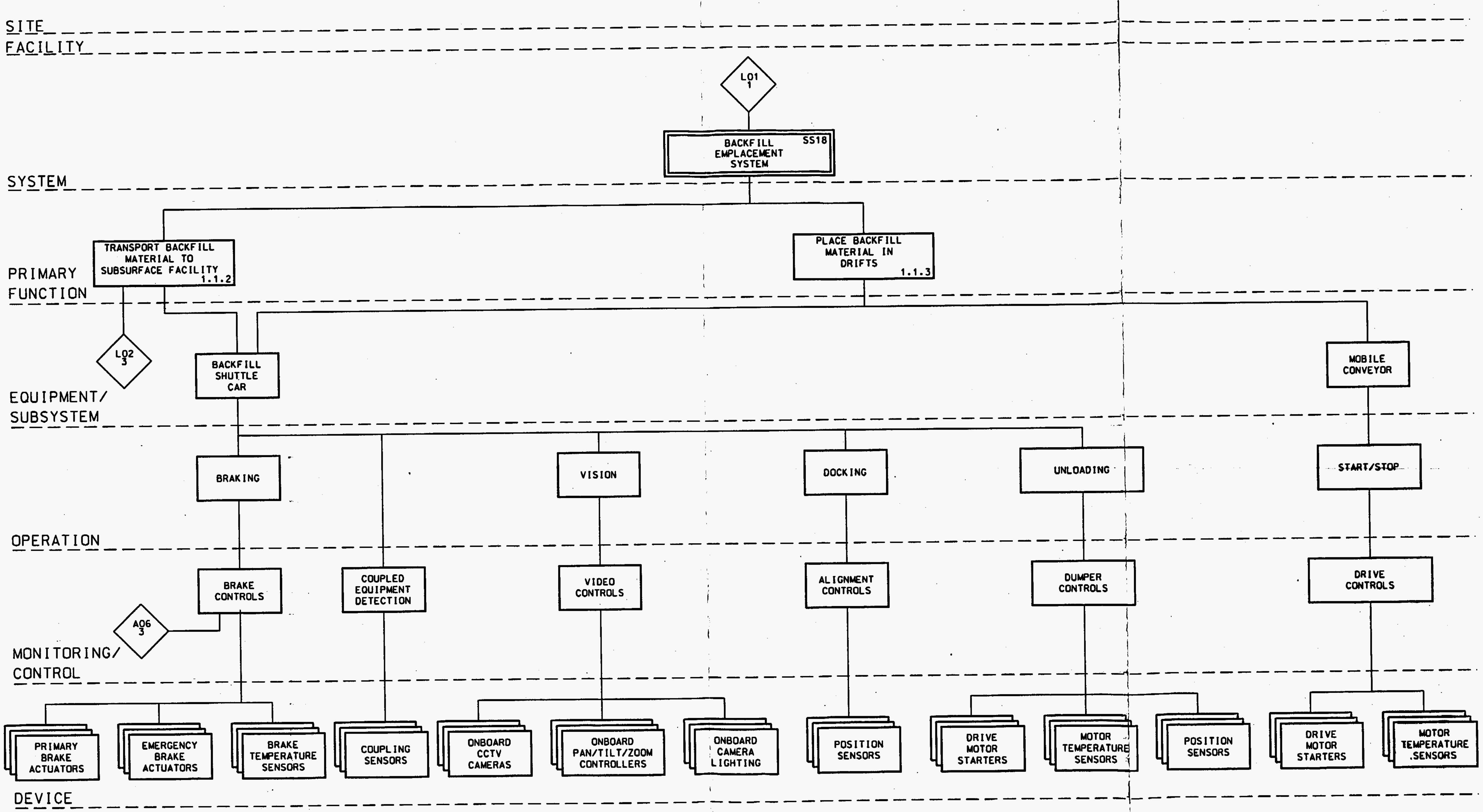
2. STACKED BOXES INDICATE MULTIPLE DEVICES/SYSTEMS

3. S/S - SUBSURFACE

t:#repss#csys#fig#sscs0104.fig

FIGURE 9
FUNCTIONAL BLOCK DIAGRAM
WASTE RETRIEVAL SYSTEM - SHT 2

FILE NAME: W03969/CSYS/FIG/SSCS0104.FIG PD: 09/24/99



LEGEND:

INTERCONNECTION POINT TO SYSTEMS ON OTHER FIGURES

XXX X —CONTINUATION IDENTIFIER NO.
—FIGURE NO.

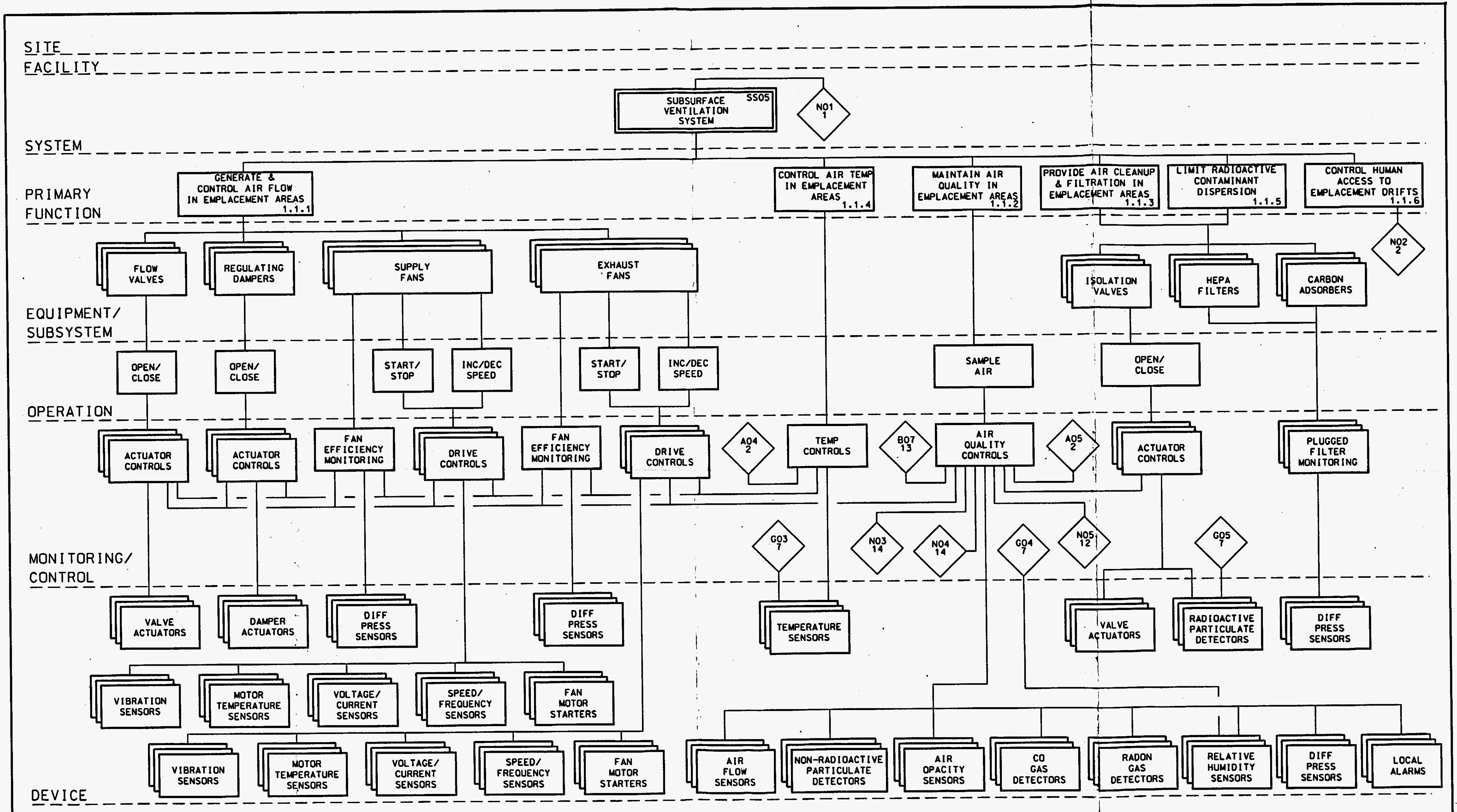
NOTES:

1. DOUBLE BOXES INDICATE PRIMARY SYSTEM DEPICTED IN THIS FIGURE.
2. STACKED BOXES INDICATE MULTIPLE DEVICES/SYSTEMS
3. S/S – SUBSURFACE

t:#repss#csys#fig#sscs0105.fig

FIGURE 10
FUNCTIONAL BLOCK DIAGRAM
BACKFILL EMPLACEMENT SYSTEM

FILE NAME: W03969/CSYS/FIG/SSCS0105.FIG PD: 08/31/99



LEGEND:

INTERCONNECTION POINT TO SYSTEMS ON OTHER FIGURES

XXX X —CONTINUATION IDENTIFIER NO.
—FIGURE NO.

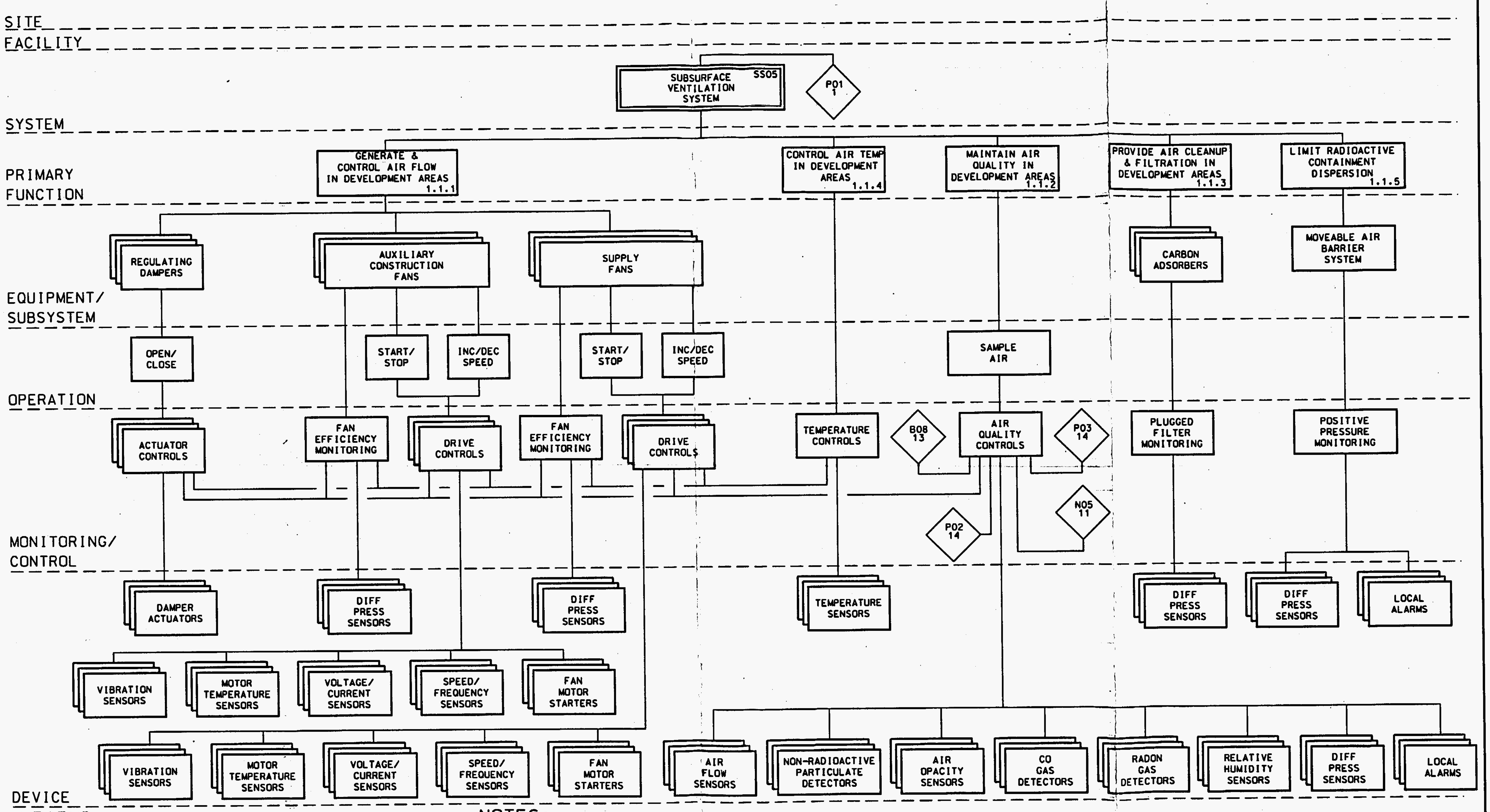
NOTES:

1. DOUBLE BOXES INDICATE PRIMARY SYSTEM DEPICTED IN THIS FIGURE.
2. STACKED BOXES INDICATE MULTIPLE DEVICES/SYSTEMS
3. S/S - SUBSURFACE

t:#repss#csys#fig#sscs0106.fig

FIGURE 11
FUNCTIONAL BLOCK DIAGRAM
SUBSURFACE VENT-EMPLACE AREAS

FILE NAME: W03969/CSYS/FIG/SSCS0106.FIG PD: 09/24/99



LEGEND:

INTERCONNECTION POINT TO SYSTEMS ON OTHER FIGURES

XXX —CONTINUATION IDENTIFIER NO.
X —FIGURE NO.

NOTES:

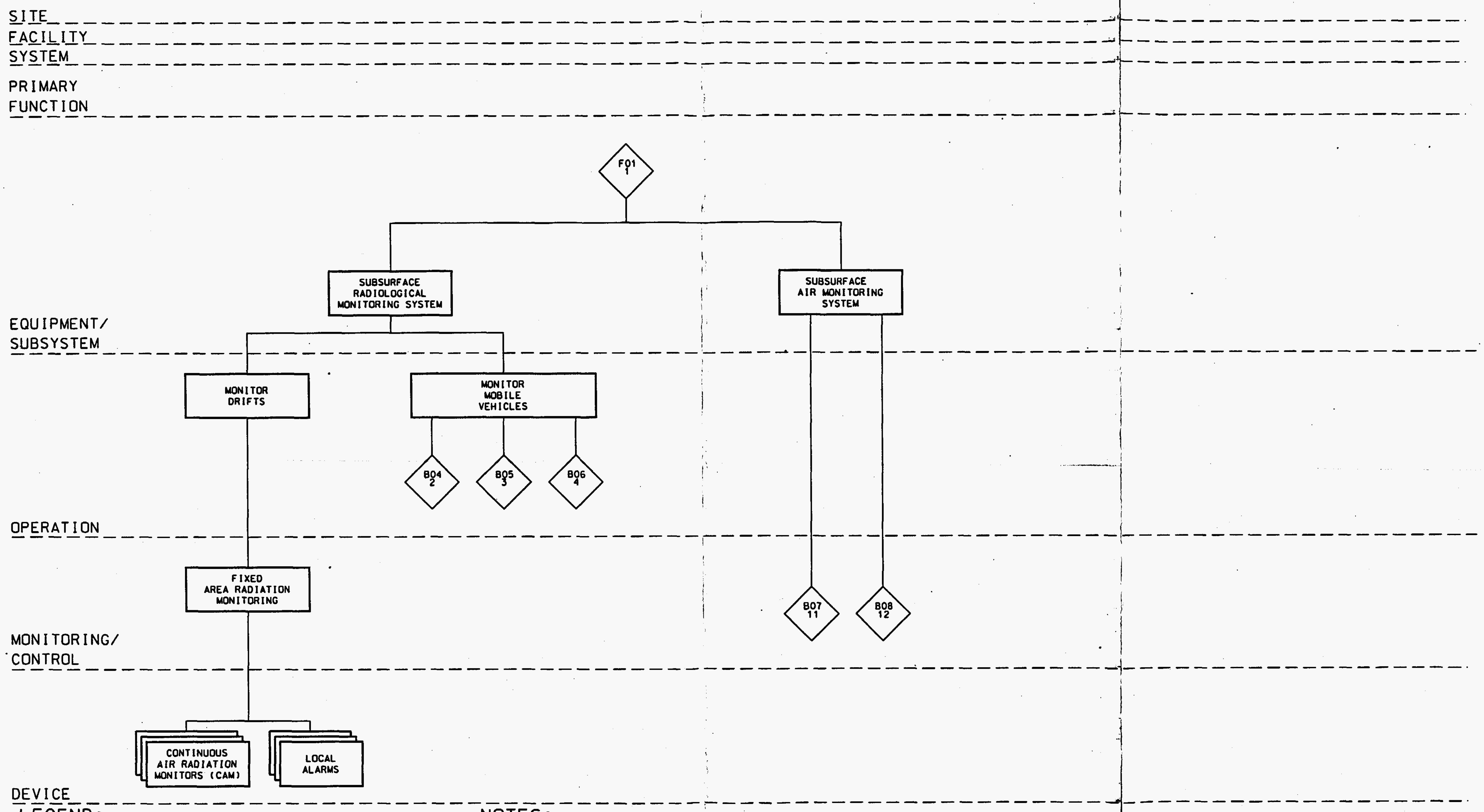
1. DOUBLE BOXES INDICATE PRIMARY SYSTEM DEPICTED IN THIS FIGURE.

2. STACKED BOXES INDICATE MULTIPLE DEVICES/SYSTEMS

3. S/S – SUBSURFACE

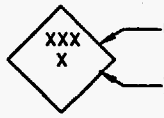
t:#repss#csys#fig#sscs0107.fig

FIGURE 12
FUNCTIONAL BLOCK DIAGRAM
SUBSURFACE VENT-DEVELOP AREAS



LEGEND:

INTERCONNECTION POINT TO SYSTEMS ON OTHER FIGURES



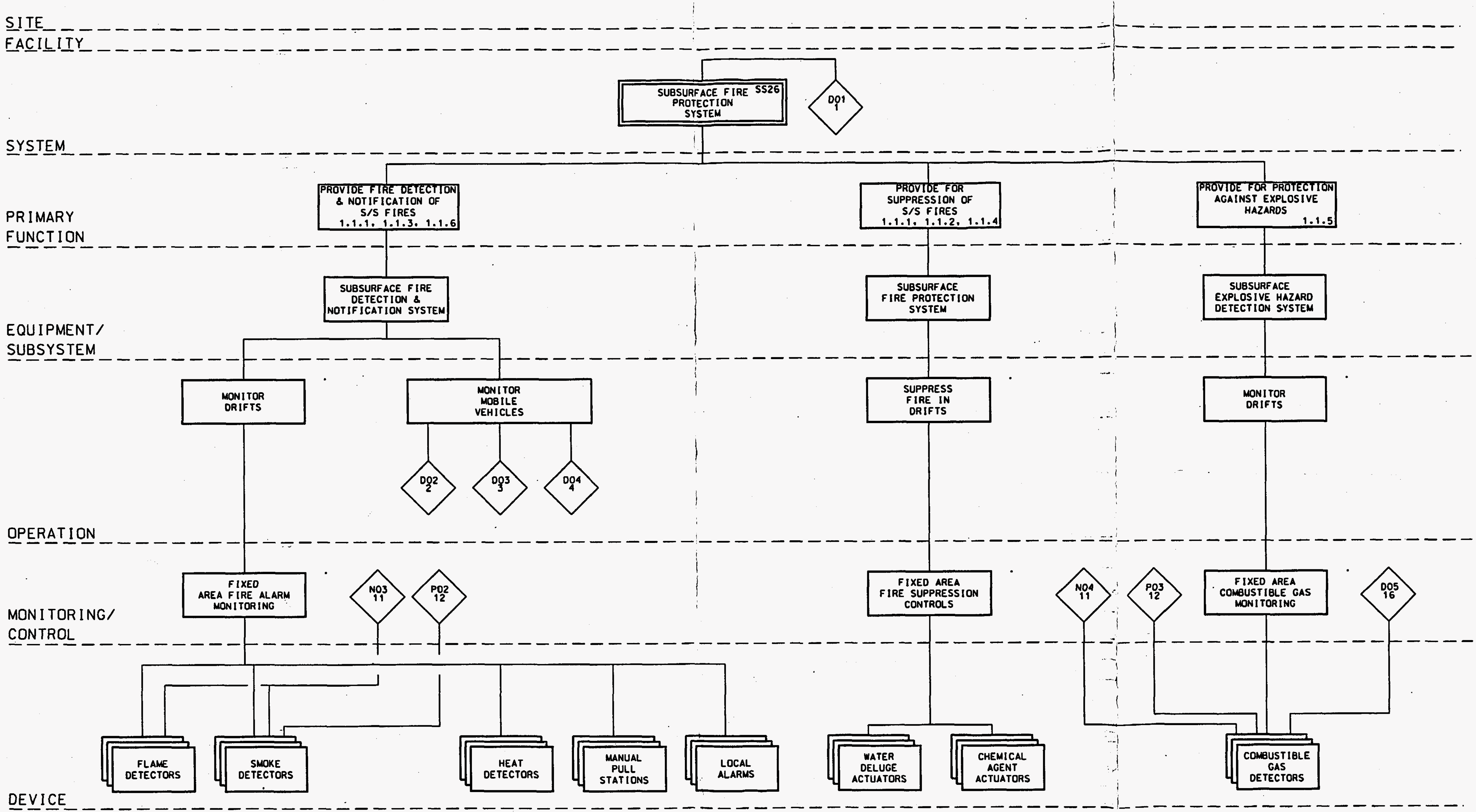
NOTES:

1. DOUBLE BOXES INDICATE PRIMARY SYSTEM DEPICTED IN THIS FIGURE.
2. STACKED BOXES INDICATE MULTIPLE DEVICES/SYSTEMS
3. S/S - SUBSURFACE

t:*repss*csys*fig*sscs0108.fig

FIGURE 13
FUNCTIONAL BLOCK DIAGRAM
SUBSURFACE RADIATION & AIR MON.

FILE NAME: W03969/CSYS/FIG/SSCS0108.FIG PD: 09/24/99


SITE
FACILITY
SUBSURFACE FIRE PROTECTION SYSTEM SS26
D01 1
SYSTEM
PROVIDE FIRE DETECTION & NOTIFICATION OF S/S FIRES 1.1.1, 1.1.3, 1.1.6
PROVIDE FOR SUPPRESSION OF S/S FIRES 1.1.1, 1.1.2, 1.1.4
PROVIDE FOR PROTECTION AGAINST EXPLOSIVE HAZARDS 1.1.5
PRIMARY FUNCTION
SUBSURFACE FIRE DETECTION & NOTIFICATION SYSTEM
SUBSURFACE FIRE PROTECTION SYSTEM
SUBSURFACE EXPLOSIVE HAZARD DETECTION SYSTEM
EQUIPMENT/ SUBSYSTEM
MONITOR DRIFTS
MONITOR MOBILE VEHICLES
SUPPRESS FIRE IN DRIFTS
MONITOR DRIFTS
D02 2
D03 3
D04 4
OPERATION
FIXED AREA FIRE ALARM MONITORING
N03 11
P02 12
FIXED AREA FIRE SUPPRESSION CONTROLS
N04 11
P03 12
FIXED AREA COMBUSTIBLE GAS MONITORING
D05 16
MONITORING/ CONTROL
FLAME DETECTORS
SMOKE DETECTORS
HEAT DETECTORS
MANUAL PULL STATIONS
LOCAL ALARMS
WATER DELUGE ACTUATORS
CHEMICAL AGENT ACTUATORS
COMBUSTIBLE GAS DETECTORS
DEVICE

LEGEND:

INTERCONNECTION POINT TO
SYSTEMS ON OTHER FIGURES

XXX X —CONTINUATION IDENTIFIER NO.
—FIGURE NO.

NOTES:

1. DOUBLE BOXES INDICATE PRIMARY SYSTEM DEPICTED IN THIS FIGURE.

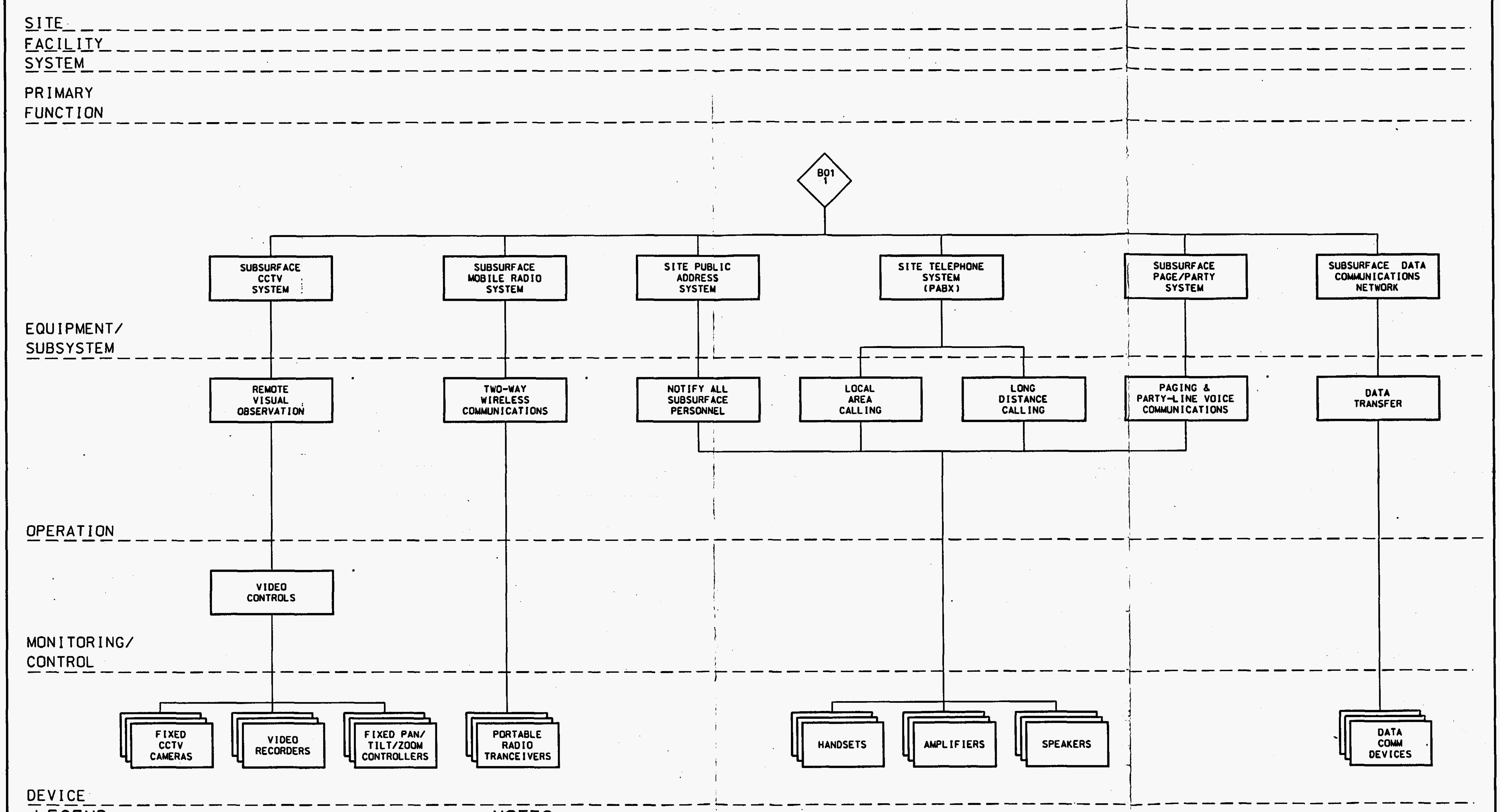
2. STACKED BOXES INDICATE MULTIPLE DEVICES/SYSTEMS

3. S/S - SUBSURFACE

t:#repss#csys#fig#sscs0109.fig

FIGURE 14
FUNCTIONAL BLOCK DIAGRAM
SUBSURFACE FIRE PROTECT SYS

FILE NAME: W03969/CSYS/FIG/SSCS0109.FIG PD: 09/24/99


SITE
FACILITY
SYSTEM
PRIMARY FUNCTION
B01 1
SUBSURFACE CCTV SYSTEM
SUBSURFACE MOBILE RADIO SYSTEM
SITE PUBLIC ADDRESS SYSTEM
SITE TELEPHONE SYSTEM (PABX)
SUBSURFACE PAGE/PARTY SYSTEM
SUBSURFACE DATA COMMUNICATIONS NETWORK
EQUIPMENT/ SUBSYSTEM
REMOTE VISUAL OBSERVATION
TWO-WAY WIRELESS COMMUNICATIONS
NOTIFY ALL SUBSURFACE PERSONNEL
LOCAL AREA CALLING
LONG DISTANCE CALLING
PAGING & PARTY-LINE VOICE COMMUNICATIONS
DATA TRANSFER
OPERATION
VIDEO CONTROLS
MONITORING/ CONTROL
FIXED CCTV CAMERAS
VIDEO RECORDERS
FIXED PAN/ TILT/ZOOM CONTROLLERS
PORTABLE RADIO TRANCEIVERS
HANDSETS
AMPLIFIERS
SPEAKERS
DATA COMM DEVICES
DEVICE

## LEGEND:

INTERCONNECTION POINT TO
SYSTEMS ON OTHER FIGURES

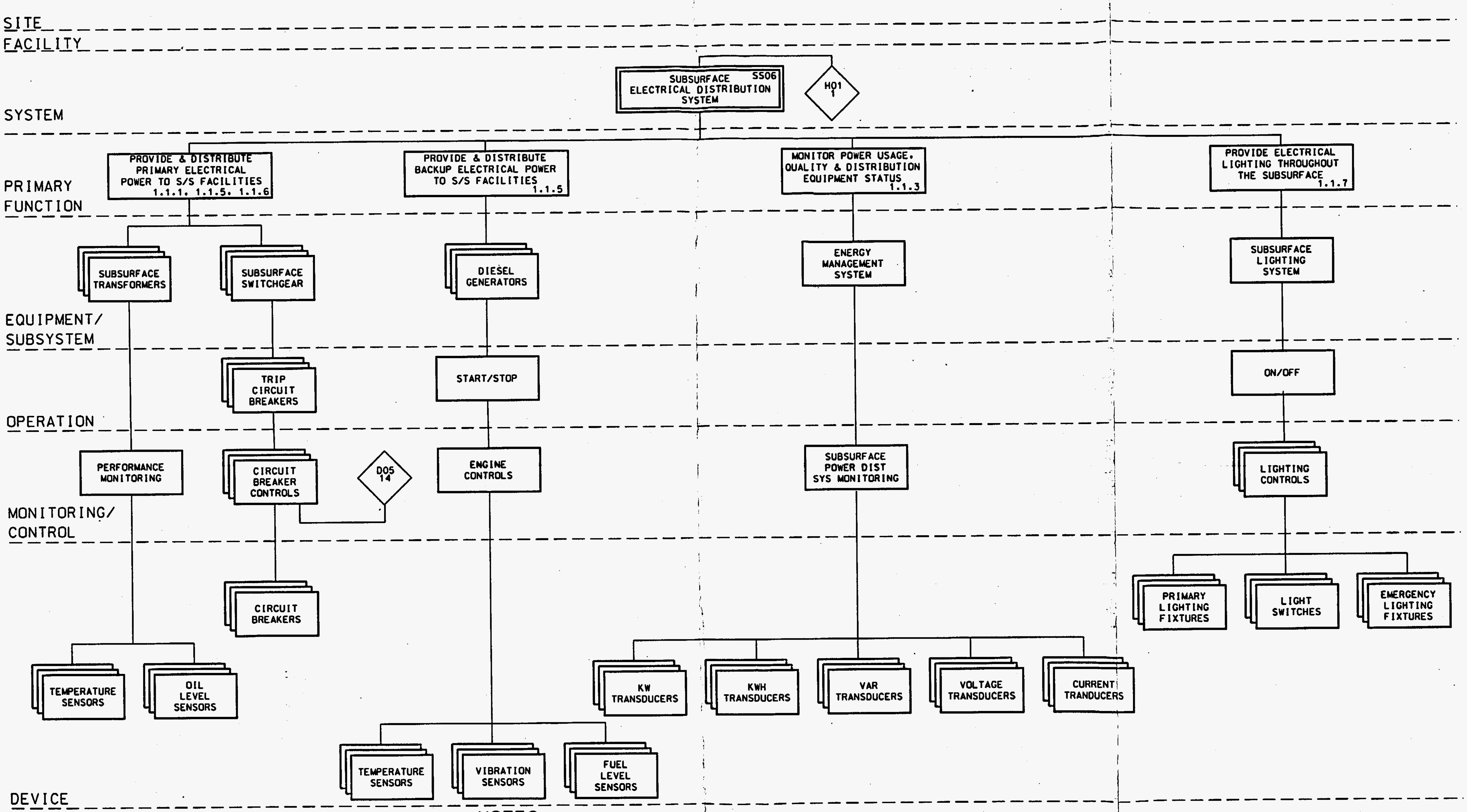
XXX
X
—CONTINUATION IDENTIFIER NO.
—FIGURE NO.

## NOTES:

1. DOUBLE BOXES INDICATE PRIMARY SYSTEM DEPICTED IN THIS FIGURE.
2. STACKED BOXES INDICATE MULTIPLE DEVICES/SYSTEMS
3. S/S - SUBSURFACE

t:#repss#csys#fig#sscs0110.fig

FIGURE 15
FUNCTIONAL BLOCK DIAGRAM
SUBSURFACE COMMUNICATIONS



## LEGEND:

INTERCONNECTION POINT TO
SYSTEMS ON OTHER FIGURES

XXX X —CONTINUATION IDENTIFIER NO.
—FIGURE NO.

## NOTES:

1. DOUBLE BOXES INDICATE PRIMARY SYSTEM DEPICTED IN THIS FIGURE.

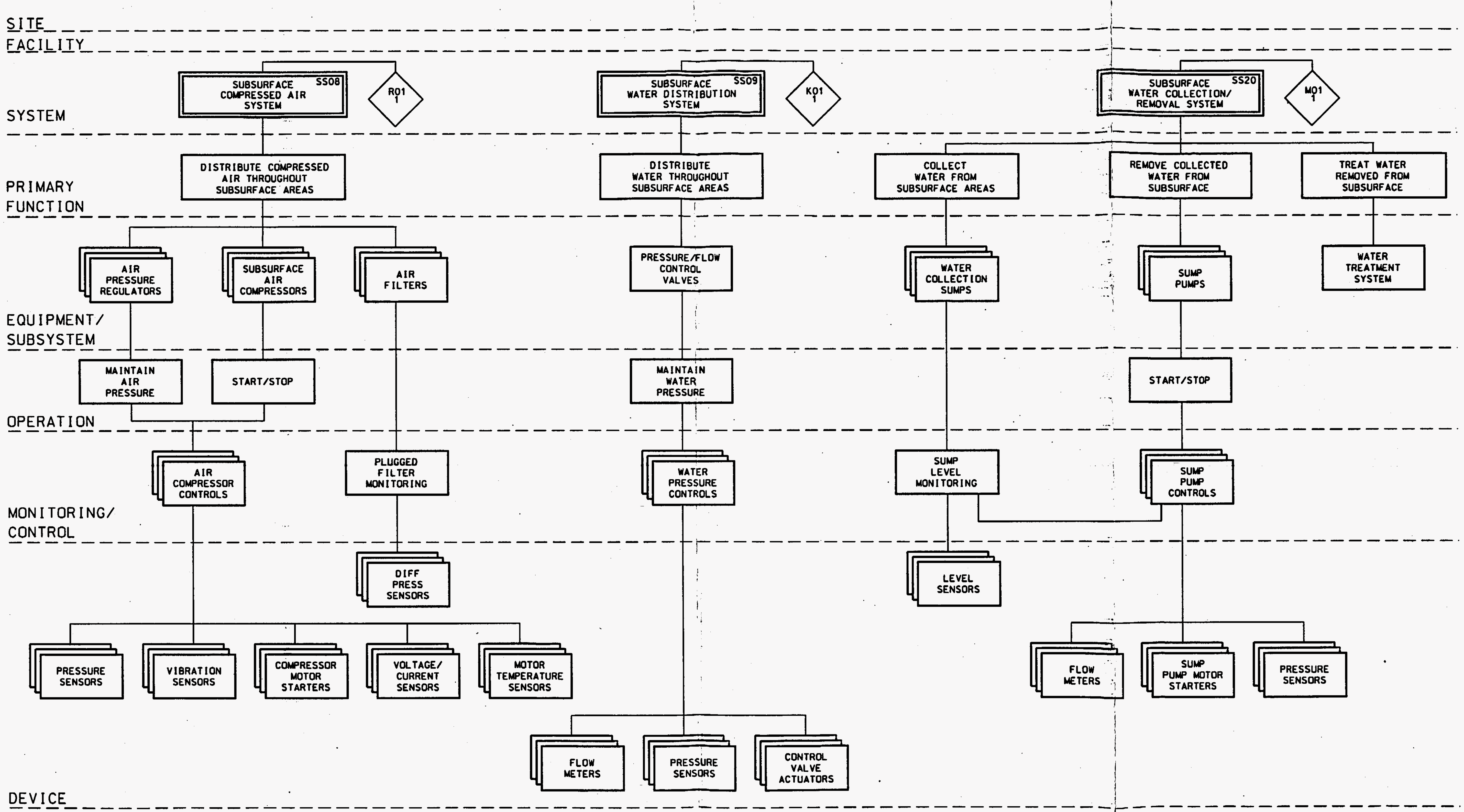
2. STACKED BOXES INDICATE MULTIPLE DEVICES/SYSTEMS

3. S/S - SUBSURFACE

t:#repss#csys#fig#sscs0111.fig

FIGURE 16
FUNCTIONAL BLOCK DIAGRAM
SUBSURFACE ELECTRICAL DIST SYS

FILE NAME: W03969/CSYS/FIG/SSCS0111.FIG PD: 09/24/99



LEGEND:

INTERCONNECTION POINT TO
SYSTEMS ON OTHER FIGURES

XXX X —CONTINUATION IDENTIFIER NO.
—FIGURE NO.

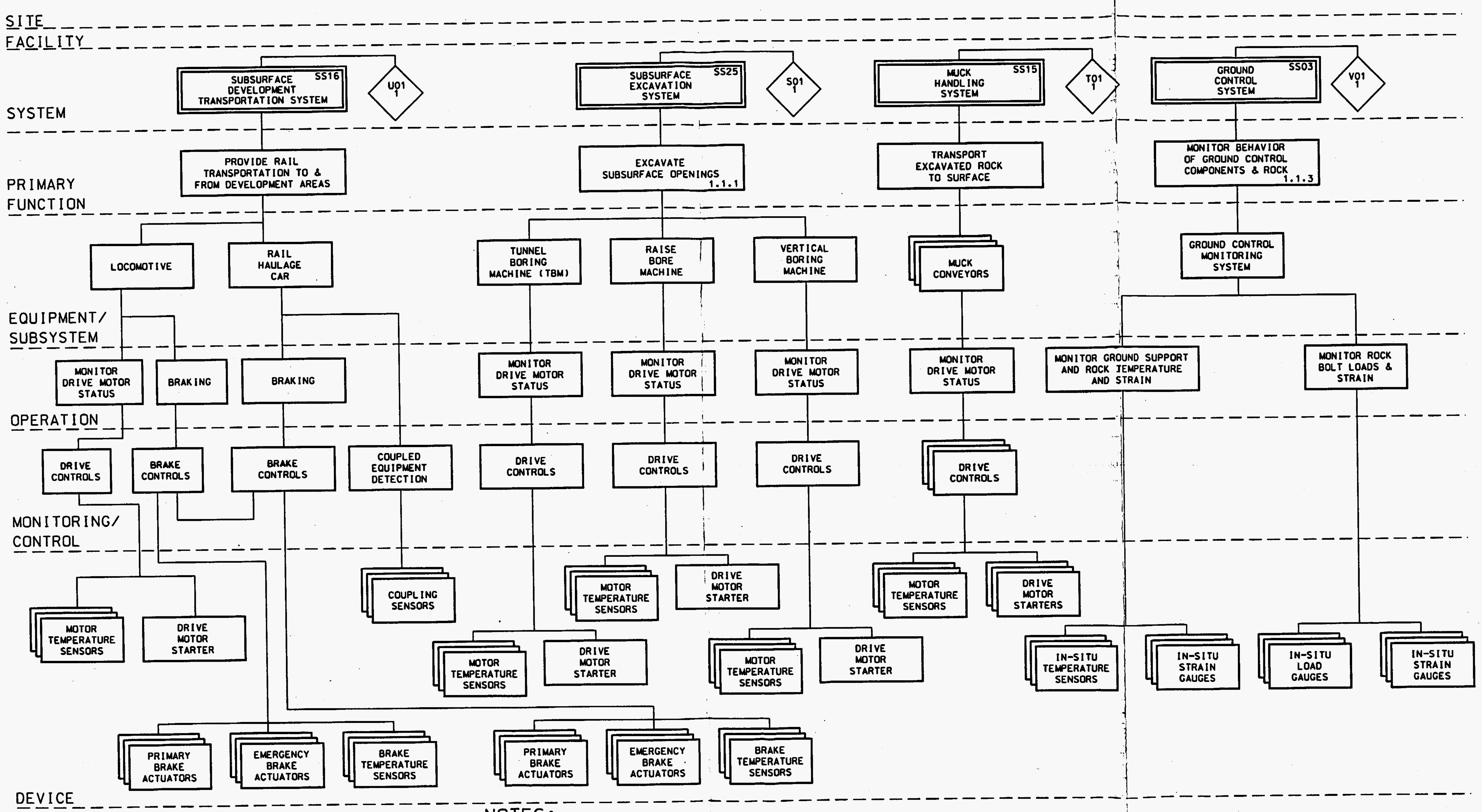
NOTES:

1. DOUBLE BOXES INDICATE PRIMARY SYSTEM DEPICTED IN THIS FIGURE.
2. STACKED BOXES INDICATE MULTIPLE DEVICES/SYSTEMS
3. S/S - SUBSURFACE

t:*repss*csys*fig*sscs0112.fig

FIGURE 17
FUNCTIONAL BLOCK DIAGRAM
SUBSURFACE UTILITIES

FILE NAME: WD3969/CSYS/FIG/SSCS0112.FIG PD: 09/24/99


SITE
FACILITY
SYSTEM
PRIMARY FUNCTION
EQUIPMENT/ SUBSYSTEM
OPERATION
MONITORING/ CONTROL
DEVICE
SUBSURFACE DEVELOPMENT TRANSPORTATION SYSTEM SS16
U01 1
SUBSURFACE EXCAVATION SYSTEM SS25
S01 1
MUCK HANDLING SYSTEM SS15
T01 1
GROUND CONTROL SYSTEM SS03
V01 1
PROVIDE RAIL TRANSPORTATION TO & FROM DEVELOPMENT AREAS
EXCAVATE SUBSURFACE OPENINGS 1.1.1
TRANSPORT EXCAVATED ROCK TO SURFACE
MONITOR BEHAVIOR OF GROUND CONTROL COMPONENTS & ROCK 1.1.3
LOCOMOTIVE
RAIL HAULAGE CAR
TUNNEL BORING MACHINE (TBM)
RAISE BORE MACHINE
VERTICAL BORING MACHINE
MUCK CONVEYORS
GROUND CONTROL MONITORING SYSTEM
MONITOR DRIVE MOTOR STATUS
BRAKING
BRAKING
MONITOR DRIVE MOTOR STATUS
MONITOR DRIVE MOTOR STATUS
MONITOR DRIVE MOTOR STATUS
MONITOR DRIVE MOTOR STATUS
MONITOR GROUND SUPPORT AND ROCK TEMPERATURE AND STRAIN
MONITOR ROCK BOLT LOADS & STRAIN
DRIVE CONTROLS
BRAKE CONTROLS
BRAKE CONTROLS
COUPLED EQUIPMENT DETECTION
DRIVE CONTROLS
DRIVE CONTROLS
DRIVE CONTROLS
DRIVE CONTROLS
MOTOR TEMPERATURE SENSORS
DRIVE MOTOR STARTER
COUPLING SENSORS
MOTOR TEMPERATURE SENSORS
DRIVE MOTOR STARTER
MOTOR TEMPERATURE SENSORS
DRIVE MOTOR STARTER
MOTOR TEMPERATURE SENSORS
DRIVE MOTOR STARTER
MOTOR TEMPERATURE SENSORS
DRIVE MOTOR STARTERS
IN-SITU TEMPERATURE SENSORS
IN-SITU STRAIN GAUGES
IN-SITU LOAD GAUGES
IN-SITU STRAIN GAUGES
PRIMARY BRAKE ACTUATORS
EMERGENCY BRAKE ACTUATORS
BRAKE TEMPERATURE SENSORS
PRIMARY BRAKE ACTUATORS
EMERGENCY BRAKE ACTUATORS
BRAKE TEMPERATURE SENSORS

LEGEND:

INTERCONNECTION POINT TO SYSTEMS ON OTHER FIGURES

XXX X —CONTINUATION IDENTIFIER NO.
—FIGURE NO.

NOTES:

1. DOUBLE BOXES INDICATE PRIMARY SYSTEM DEPICTED IN THIS FIGURE.

2. STACKED BOXES INDICATE MULTIPLE DEVICES/SYSTEMS

3. S/S - SUBSURFACE

t:*repss*csys*fig*sscs0113.fig

FIGURE 18
FUNCTIONAL BLOCK DIAGRAM
SUBSURFACE CONSTRUCT DEVELOP SYS

FILE NAME: W03969/CSYS/FIG/SSCS0113.FIG PD: 09/24/99

## 6.3 SUBSURFACE REPOSITORY INTEGRATED CONTROL SYSTEM PHYSICAL ARCHITECTURE

This section examines a preliminary target configuration of a physical architecture for the Subsurface Repository Integrated Control System. The target configuration will be dynamic and will be evolving over time in order to accommodate additional design details, changes in repository design concepts, and changes in available technology.

### 6.3.1 Physical Architecture: Definition, Purpose, and Approach

The physical architecture for the Subsurface Repository Integrated Control System is represented by a schematic of the overall process monitoring/control and communications systems. It provides the design development team with a high-level view of system and subsystem components, describes system connectivity, establishes boundaries and the link relationships of components to each other, and allows the development team to visualize the various communication paths and data flow between systems and components. The architecture also allows an observer to visualize how the electronic systems and components will map onto the physical facility being designed and illustrates how the functions previously defined in the functional block diagrams will be accomplished with the physical hardware. The physical architecture also serves as the foundation for determining the detailed physical layout of the Subsurface Repository Integrated Control System.

The physical architecture basically consists of process control and communication hardware components connected together and distributed over several vertical "layers." The layers show a network hierarchy, ranging from two supervisory layers through a monitoring/control layer and eventually reaching the lowest level, which is called the process layer. The frequency of communication (see Section 6.3.1.5) and volume of data usually increases as one moves downward and into the monitoring/control layer. The components and systems on the monitoring/control layer are usually the busiest because it is at this level that the routine data acquisition and control activities take place. Also, the quantity of data being communicated decreases as one moves upward through the various layers. Only a limited amount of data reaches the highest level due to the decreased need for process monitoring and control information at this point in the hierarchy. Therefore, given the overall distribution of data, the network must operate at increasing greater speeds in moving from the higher to the lower levels of the network.

Generally, the physical architecture equipment at the monitoring/control and process layers carries out the activities described by the functional block diagrams at their monitoring/control and device levels (Section 6.2, Figures 1 through 18), and communicates process information to other levels of the network hierarchy to achieve integrated monitoring and control. With respect to the functional block diagrams, the physical architecture identifies and describes the hardware components and their physical connections within a hierarchical network structure for process monitoring, control, and communications.

The physical architecture layout design presented herein is preliminary and conceptual in nature. It is likely that detailed refinements will arise from further analysis of that presented.

The primary factors considered in the design of the physical architecture are described in the sections below.

#### 6.3.1.1 Data Communications Connectivity

The physical architecture must provide connectivity between the various systems and subsystems. Design consideration must be given to ensure that the routing of various communication media for a network is inclusive of all nodes requiring network services. Furthermore, if two independent control systems located on different networks must share or exchange information, a communication path must be available between the two networks; either as a direct path between the two or as a path routed across other networks.

#### 6.3.1.2 Network Bandwidth and Throughput

The network bandwidth is essentially the capacity of the network. It is determined by the maximum amount of traffic that will pass through the network in a given time period. The throughput is an end-to-end measurement that includes the data communications equipment (and its limitations) as a factor in determining the overall bandwidth. Bandwidth is a critical issue because it determines how much information can be transmitted in a timely fashion. The frequency and quantity of information the network is expected to handle dictates the necessary bandwidth required of the network.

#### 6.3.1.3 Network Segmentation

Segmentation is the tool that is used to properly balance the networks and traffic flow. In some cases, busy networks must be separated to allow more efficient bandwidth (or capacity) utilization, and at the same time must be logically united to allow traffic to flow to and from a particular segment so that communication between devices is accomplished on demand. Segmentation also allows logical separation of devices when communication is not needed, i.e., when a particular device is not required to receive certain information.

#### 6.3.1.4 Redundancy

Redundancy in equipment, physical transmission media (wire, fiber optic cable, etc.), and systems is an important consideration in design. The concepts of spares, alternate paths, and diverse authority are represented in redundancy. The theory is simple: if something fails, something else must be in place to function in its place. The design must therefore accommodate alternate paths, alternate equipment, and alternate physical media that would function in the event of a single component failure that would otherwise impact the function of multiple items within the system. Thus, a redundant system prevents common-cause failures. Redundancy issues are identified in the *Monitored Geologic Repository Instrumentation and Control System Strategy* document (DIRS 35).

#### 6.3.1.5 Data Acquisition Frequency

The frequency at which data are taken also dictates part of the design of the physical architecture. The job of the network is to get information from one node (a device or location) to another in a timely fashion. Certain segments of the network will require higher speeds (bandwidth, throughput, etc.) because of higher data acquisition frequency. The faster the data are injected into the network, the faster the network must transmit data to the destination. Because of the higher data rates at the lower levels, that network segment must be made to operate faster. At the higher levels, the network need not operate as fast for reasons stated earlier in Section 6.3.1 regarding the distribution of information throughout the network hierarchy.

#### 6.3.1.6 Determinism

A network is said to be deterministic when it can guarantee that a specific piece of data can reach its destination in a predetermined time interval. Each station can be guaranteed the right to communicate within a certain time frame. This is important for data that are time-critical. At the lower levels, where data acquisition and control takes place, a deterministic network is required. At higher levels, where administration-oriented data are transmitted, the timing is less critical and traditional LANs (local area networks) may be employed.

#### 6.3.1.7 Supervisory Functions

Flexible HMI workstation placement will be required for supervisory function. The workstations will likely be placed on both the surface and within the subsurface facility. A supervisory workstation is an overseeing authority that is not concerned with the automatic and routine operations of the facility, but can monitor various process parameters and can assume certain control and override capabilities under secured circumstances. Supervisory stations are typically connected directly to the main control networks.

#### 6.3.1.8 Administrative Functions

Administrative functions are those commonly associated with the business aspects of the facility. Typically, HMI workstations engaged in these functions would be directly connected to the higher levels of the network hierarchy. It is expected that they would have routed access to the lower network levels under secured circumstances. Access to the lower levels would be necessary to interface the business functions (e.g., production planning, inventory reconciliation, etc.) to process engineering data. Administrative access would likely be from both site and offsite locations, again, under secured circumstances. Surface administrative functions are identified in the *Site Communications and Control Systems Technical Report* (DIRS 20).

#### 6.3.1.9 Safety

Functions that are "important to safety" must be given additional consideration. Segregation and isolation from routine control functions, added redundancy, and special attention to reliability are necessary treatment measures. Safety issues are identified and discussed in the *Monitored Geologic Repository Instrumentation and Control System Strategy* document (DIRS 35).

#### 6.3.1.10 Modularity

The design of the network must lend itself to modular upgrades, and easy modification and expansion. The implementation schedule of the subsurface control systems will no doubt require modular development of the various data communication networks. Physical distances might be an associated factor. The ability to segment, add, remove, and relocate network modules as construction development proceeds is important.

#### 6.3.1.11 Maintenance

Maintenance procedures and practices must be considered. Redundant networks and alternate media paths are important, especially if any critical communications devices must be periodically removed from service for maintenance purposes.

#### 6.3.1.12 Troubleshooting

Ease of troubleshooting is an important consideration. As with any physical or electronic system, the more complex a network topology is, the more difficult and time consuming it is to troubleshoot and diagnose problems. Complexity is determined by the number of nodes on a given network as well as by the total number of networks communicating with each other.

#### 6.3.1.13 Replacement

As data communications technology evolves, the flexibility to upgrade and replace portions of the overall network is important. From preliminary design to implementation, technological advances will continuously occur.

#### 6.3.1.14 Reliability

Simplicity and redundancy can impact the reliability of a network. If these and other aspects can enhance the reliability of the communications equipment and network as a whole, such design features should be implemented. Reliability issues are identified and discussed in the *Monitored Geologic Repository Instrumentation and Control System Strategy* document (DIRS 35).

#### 6.3.1.15 Physical Distance Considerations

The large physical distances encountered in the repository require special consideration in network design. In this respect, the repository differs from other types of industrial facilities such as chemical manufacturing plants or power generating stations.

#### 6.3.1.16 Physical Media Requirements/Constraints

Before final design, an evaluation must be undertaken to consider any special environmental impact on the physical media used throughout the network infrastructure. Topics for study should include thermal and radiological effects on the transmission media and electronics equipment.

#### 6.3.1.17 Installation Requirements/Constraints

The physical routing of the network transmission media is important. For instance, media should not be routed through areas that are not designated for human access. A media failure in this area would pose a serious maintenance problem.

### 6.3.1.18 Human-Machine Interface

The HMI is an important factor to consider in the design of physical architectures. Providing efficient, convenient, and straightforward methods for humans to monitor and respond to process system operations is essential to a successful design.

Each of the above factors must be weighed and balanced against each other throughout the development stages of the design.

### 6.3.2 Physical Architecture Layer Descriptions

The following table describes the layers depicted in the physical architecture diagrams.

Table 2. Physical Architecture Layer Description

| Layer No. | Layer Name | Layer Description |
|---|---|---|
| 4 | Site Supervisory | Site Operations System supervisory hardware and software |
| 3 | Subsurface Supervisory | Subsurface Repository Integrated Control System supervisory hardware and software |
| 2 | Monitoring /Control | Process monitoring and control hardware and software |
| 1 | Process | Process I/O devices and instrumentation, and communication equipment |

### 6.3.3 Introduction to the Physical Architecture Design

A preliminary conceptual physical architecture design that integrates the various subsurface monitoring, control, and communications systems is presented in Figures 19 through 24. Section 6.4.1 should be consulted for a definition of terms used on these diagrams and throughout the following discussion of the physical architecture design. While specific types of control and communications equipment are shown on the diagrams, the final decisions concerning the exact nature of these devices will necessarily depend upon further definition of the MGR as well as on evolutionary trends among hardware and software products within the process control and data communications industries. Thus, it is understood that the process control and data communication technologies, and protocols offered by these diagrams are subject to change or refinement according to developments in the MGR design.

The physical architecture diagrams for the process control and data communications systems (represented in Figures 19 through 22) of the Subsurface Repository Integrated Control System are divided vertically into the layers named and described in Table 2. Since no preliminary physical architecture has been developed to date for site operations, no attempt has been made to depict any equipment for the site supervisory layer in these figures. However, an interface between the site supervisory and subsurface supervisory layers is represented by two data communication links from data communications equipment for the Subsurface Repository Integrated Control System to similar equipment for site operations. These links are shown in Figure 19. With respect to the monitoring/control layer of Figures 20 through 22, a variety of microprocessor-based process control equipment is shown for carrying out the various monitoring and control functions presented in the control system functional block diagrams discussed in Section 6.2. It should be pointed out that the specific equipment types and quantities shown at this layer for a typical network node for subsurface data communications are strictly conceptual. A variety of monitoring and control devices are depicted solely for the purpose of showing the types of devices currently available for the applications defined by the control system functional block diagrams.

Regarding the process layer of Figures 20 through 22, at the most basic level of the physical arrangement of the Subsurface Repository Integrated Control System, no input/output devices wired to the various controllers on the monitoring/control layer are named or shown. There are two reasons for this arrangement. The first is that the types of devices that would otherwise have been depicted here are those devices named on the device level of most of the functional diagrams. The second is that the location, arrangement, and distribution of the various motors, valves, transmitters, sensors, switches, etc., for the various systems depicted in the functional diagrams cannot be determined at what is now a preliminary stage in the design of these systems.

The layer stratification concept outlined above is not applicable with respect to the physical architecture of the Subsurface Repository Integrated Control System voice and video communication networks shown in Figures 23 and 24. Instead, the equipment proposed for the voice and video systems is shown as divided, according to location, between the subsurface operations monitoring and control room at the surface, and all other subsurface areas.

### 6.3.4 Physical Architecture Design

The physical architecture design for subsurface process data communications employs two subsurface-wide fiber distributed data interface (FDDI) local area networks (LANs) as shown in Figures 19 through 22.

As shown in Figure 20, one FDDI LAN is a single-ring network (one cable, two fibers) made up of a number of nodes that link area specific Ethernet LANs which, in turn, are connected to those subsurface process systems that this analysis considers to be of a non-critical nature with respect to safety. As shown in Figure 21, the other FDDI LAN is a dual-ring network (two cables, two fibers per cable) composed of a number of distributed nodes linking area-specific Ethernet and specialty LANs which, in turn, are connected to subsurface processes regarded as critical to safety by this analysis. In the case of the FDDI LAN for safety-critical systems, all links to the Ethernet LANs shown on the subsurface supervisory layer are doubly redundant. Furthermore, all links to personal computers (PCs), PLCs, DCSs, and other control devices shown on the monitoring/control layer are also doubly redundant. Due to the preliminary conceptual nature of the FDDI LAN network design, complete equipment/cabling redundancy requirements and details between the LAN hubs on the subsurface supervisory layer and the various input/output devices on the process layer have not been specified or fully developed.

As shown in Figure 19, what is termed "Node #1" on each of the two FDDI LANs provides a link to an Ethernet star topology LAN which, in turn, is linked to supervisory control equipment for the Subsurface Repository Integrated Control System to be housed in the Central Control Center at the surface. With the exception of the various process monitoring and control devices, this equipment corresponds to the equipment shown on the device level of the functional block diagram for the Subsurface Repository Integrated Control System (the subsurface portion of the MGR OMCS), (see Figure 1). As can be seen in Figure 19, the supervisory control equipment is grouped into supervisory consoles according to the types of process systems for which each is responsible. These systems are presented in the functional block diagrams (Figures 2 through 18) and are discussed in Sections 6.2.2.2 through 6.2.2.14.

The ventilation system supervisory console is singularly responsible for the Subsurface Ventilation System. Next, the waste transportation, emplacement, and retrieval operations supervisory console is dedicated to the Subsurface Emplacement Transportation System, the Waste Emplacement System, and the Waste Retrieval System, respectively. The supervisory console for the construction development and backfill operations oversees the Subsurface Excavation System, the Muck Handling System, the Subsurface Development Transportation System, the Ground Control System, and the Backfill Emplacement System. The utilities and energy management supervisory console is responsible for the Subsurface Compressed Air System, the Subsurface Water Distribution System, the Subsurface Water Collection System, and the Subsurface Electrical Distribution System. The performance confirmation supervisory console is dedicated to the Performance Confirmation Data Acquisition/Monitoring System and the Performance Confirmation Emplacement Drift Monitoring System. Finally, the safety and fire protection supervisory console incorporates the Subsurface Radiological and Air Monitoring Systems, and the Subsurface Fire Protection System. A control room layout for the Subsurface Repository Integrated Control System showing the proposed arrangement of these consoles is depicted in Figure 27.

Figure 22 shows Node #1 of the non-safety-critical FDDI LAN linked to a leaky feeder network that extends throughout the subsurface facility for radio-based data and video communications to and from remotely operated rail vehicles. A leaky feeder system is a radio-based communication system which utilizes a dedicated signal transmission cable called a leaky feeder. It is composed of a number of unidirectional radio frequency bands carried on a repeater network. The coaxial cable has partial shielding allowing only selected radio signals to "leak" from and to the cable. This same leaky feeder network is represented in Figure 23, where it is also used for radio-based voice communications among personnel working underground, and between these personnel and subsurface operations control room operators. The subsurface voice-radio communications system also provides for a radio link with surface and site operations personnel via a base station transceiver with a fixed antenna located at the subsurface surveillance and security console within the control room for the Subsurface Repository Integrated Control System. It is intended that a number of hand-held transceivers (located within the same control room) offering similar communications capabilities will be distributed for operator use among the various other supervisory consoles.

Figures 23 and 24 show the subsurface wire-based voice communication systems and the subsurface video monitoring systems, respectively. Although today's communications technologies provide for the propagation of voice, data, and video signals over a single network, the maximum number of individual channels available for each signal type is severely limited, at the present time, due to the bandwidth constraints of integrated systems. Thus, in an attempt to preserve flexibility with respect to upper limits on the number of communication channels (attached devices), a more conventional network design is presented for the voice and video communication systems. In this design, data, voice, and video communications are configured across separate networks. Furthermore, all communication and monitoring devices (or groups of such devices) are shown as individually wired from a central distribution point. Therefore, this configuration is subject to a significant change in network design as bandwidth technology improves for short-distance communication applications in harsh industrial environments.

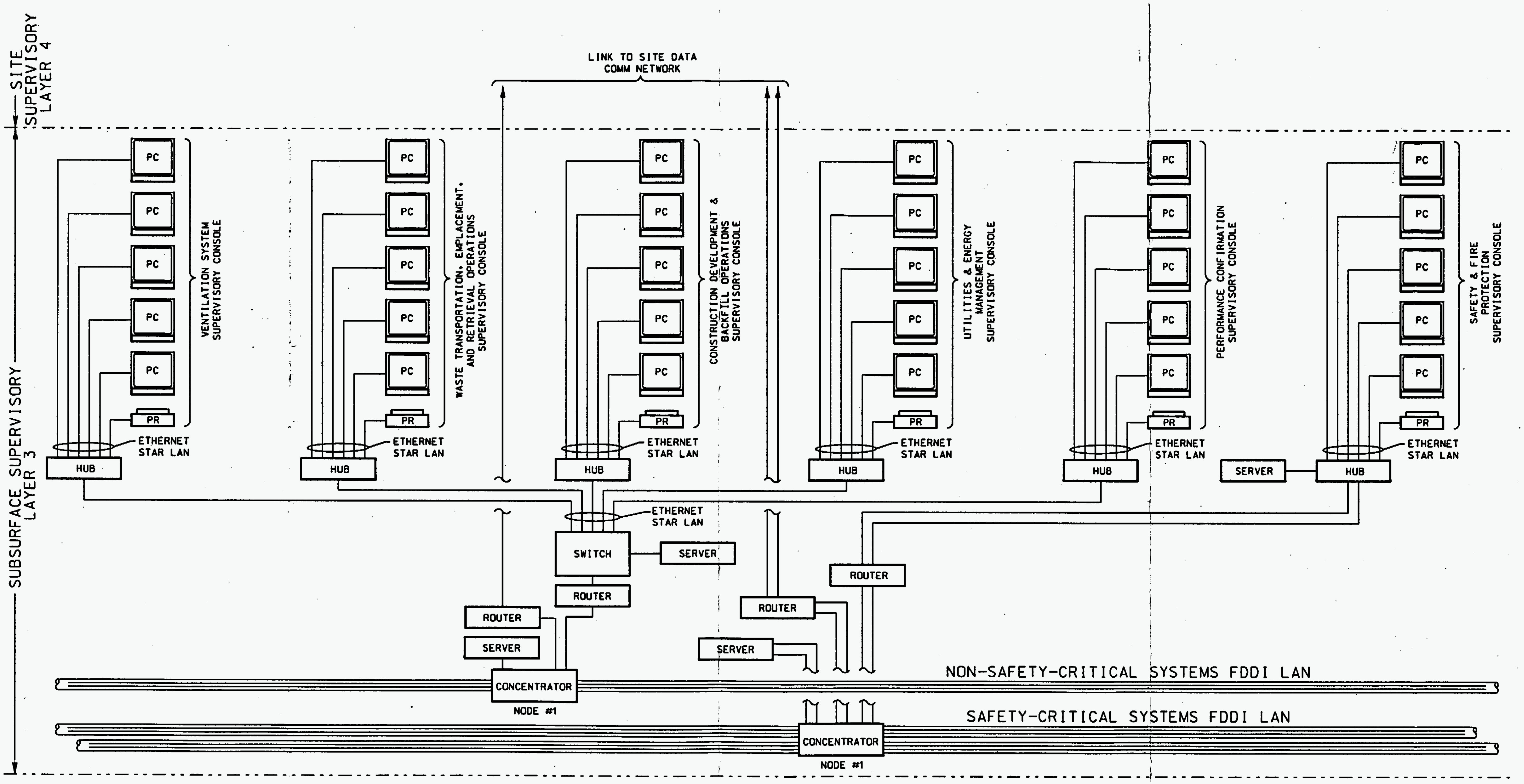
Clearly, the number of page/party system zones (and the number of devices attached to each zone) will depend upon the number and locations of subsurface areas requiring immediate access to voice communications equipment. A similar situation exists with respect to the number of video cameras distributed throughout the subsurface. As shown in Figure 24, a number of video monitors are grouped together and housed in what is called the subsurface surveillance and security console. The number of video monitors for subsurface surveillance purposes will primarily be determined by the total number of video cameras that will be required.

An in-depth discussion of the data communication technologies employed throughout the physical architecture is presented in Section 6.4.

### 6.3.5 Physical Architecture Summary

The evolving components of computer technology, together with innovative developments in process instrumentation, are forcing process control system manufacturers to introduce new products and related technologies at an unprecedented rate. This exploding growth in technology is rendering today's process instrumentation and control systems obsolete in just a few years. The maturing of non-proprietary or "open system" standards and manufacturer compliance with them will improve flexibility and reliability, and should lower costs. An open system design allows computer-based devices of various types from different manufacturers to communicate with one another in accordance with a publicly available standard for data encoding/decoding. Because of rapidly evolving control system technologies, the physical architecture design proposed in this document is to be considered preliminary and should not be understood to serve as the definitive solution for the Subsurface Repository Integrated Control System. It does, however, reflect much of today's "state of the art" in the process controls industry, and can be used as the starting point for detailed design and the development of documents for cost estimating, planning, etc. It will be necessary to monitor regulatory requirements and work closely with major control system product manufacturers to update the emerging control system design if the project schedule and expected license application requirements are to be met.

FILE NAME: W03969/CSYS/FIG/SSCS0115.FIG PD: 09/24/99


SITE SUPERVISORY LAYER 4
SUBSURFACE SUPERVISORY LAYER 3
LINK TO SITE DATA COMM NETWORK
PC
PR
HUB
ETHERNET STAR LAN
VENTILATION SYSTEM SUPERVISORY CONSOLE
WASTE TRANSPORTATION, EMPLACEMENT, AND RETRIEVAL OPERATIONS SUPERVISORY CONSOLE
CONSTRUCTION DEVELOPMENT & BACKFILL OPERATIONS SUPERVISORY CONSOLE
UTILITIES & ENERGY MANAGEMENT SUPERVISORY CONSOLE
PERFORMANCE CONFIRMATION SUPERVISORY CONSOLE
SAFETY & FIRE PROTECTION SUPERVISORY CONSOLE
SERVER
SWITCH
ROUTER
CONCENTRATOR
NODE #1
NON-SAFETY-CRITICAL SYSTEMS FDDI LAN
SAFETY-CRITICAL SYSTEMS FDDI LAN

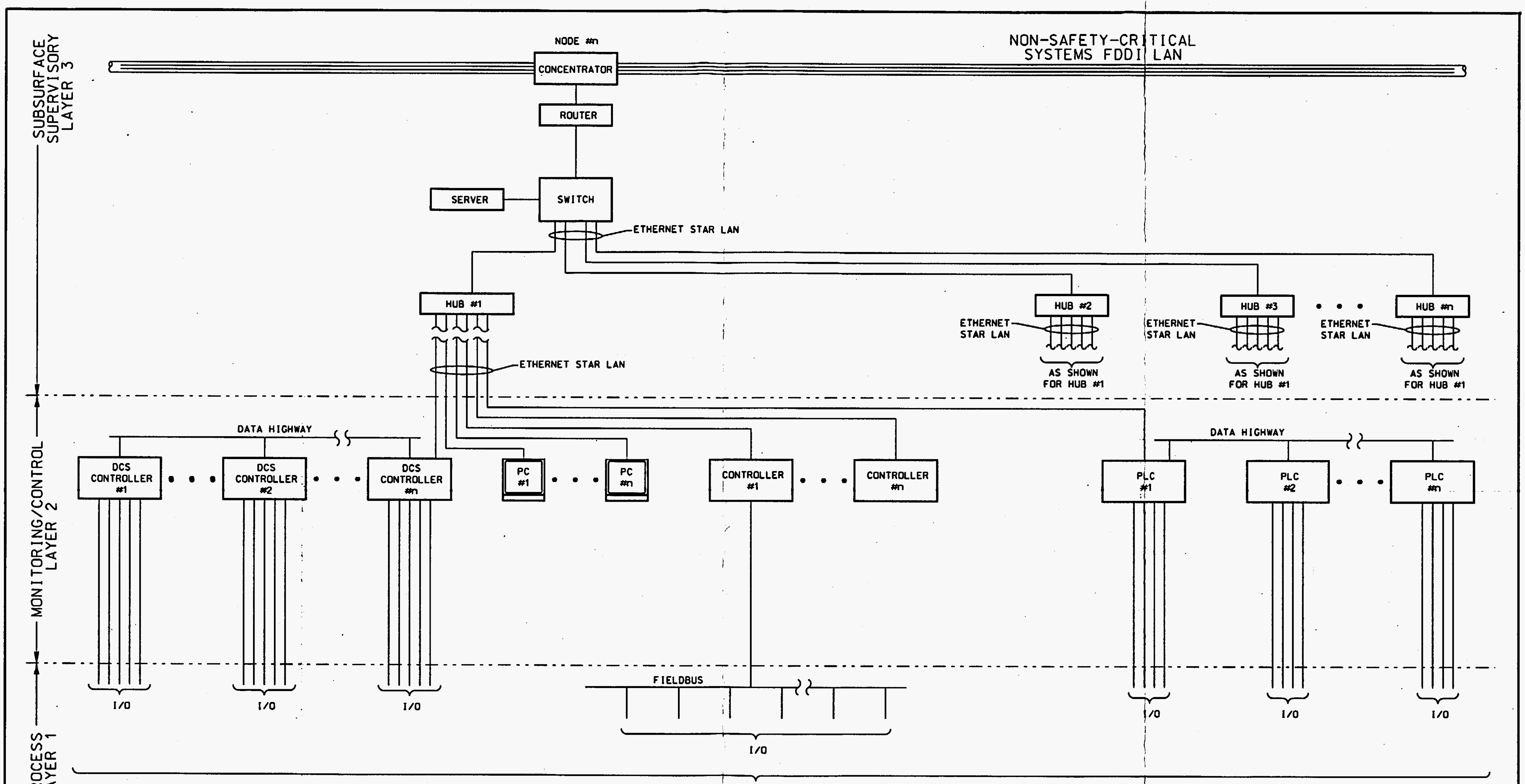
LEGEND:

DCS - DISTRIBUTED CONTROL SYSTEM
I/O - INPUT/OUTPUT
MON - VIDEO MONITOR
MUX - MULTIPLEXER
PA - PUBLIC ADDRESS
PABX - PRIVATE AUTOMATIC BRANCH EXCHANGE
PC - PERSONAL COMPUTER (HMI WORKSTATION)
PLC - PROGRAMMABLE LOGIC CONTROLLER
PR - PRINTER
RF - RADIO FREQUENCY

t:*repss*csys*fig*sscs0115.fig

FIGURE 19
SUBSURFACE REP INT CONTROL SYS
PHYSICAL ARCH DIAG - SHT 1

FILE NAME: W03969/CSYS/FIG/SSCS0116.FIG PD: 09/24/99



LEGEND:

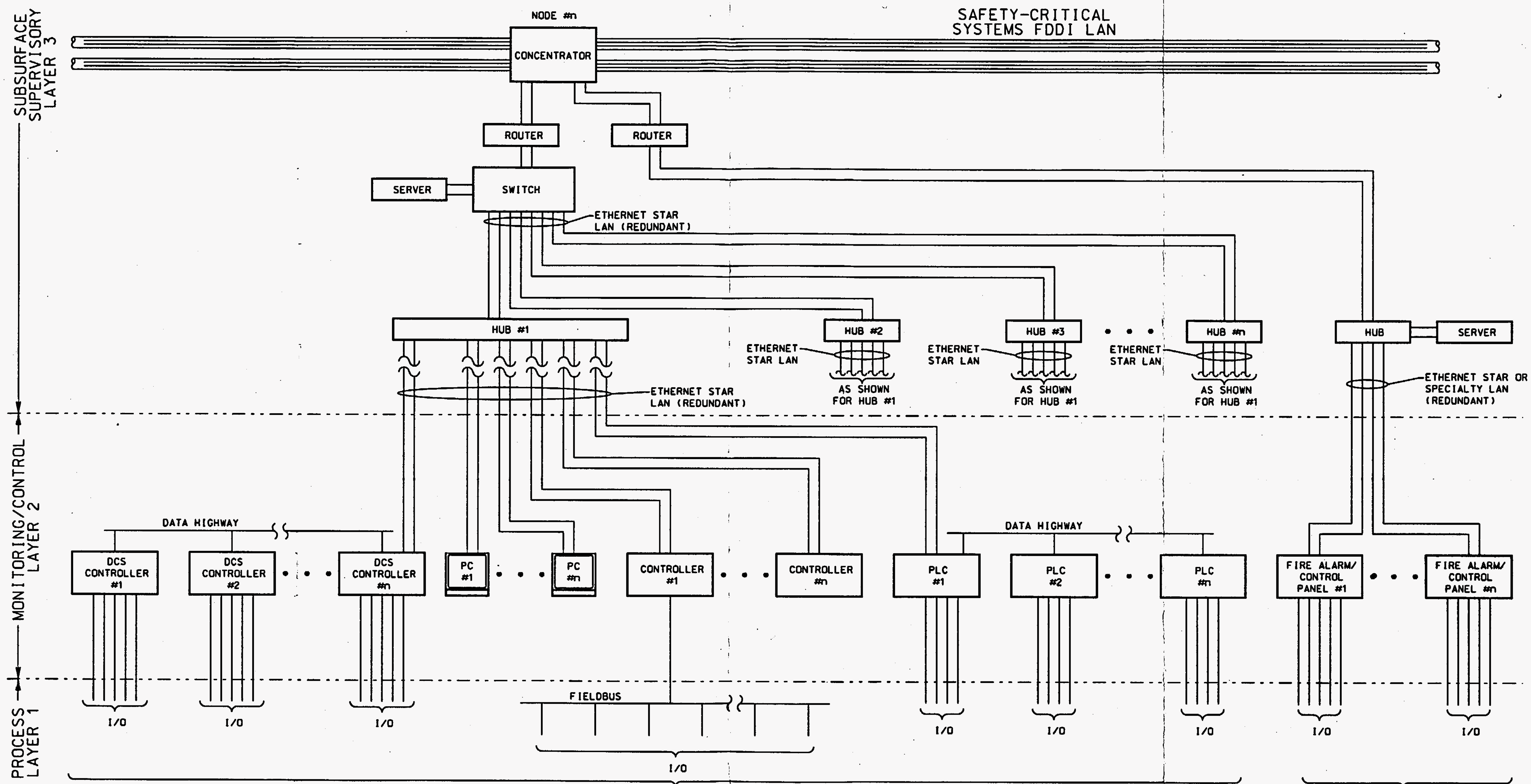
DCS - DISTRIBUTED CONTROL SYSTEM
I/O - INPUT/OUTPUT
MON - VIDEO MONITOR
MUX - MULTIPLEXER
PA - PUBLIC ADDRESS
PABX - PRIVATE AUTOMATIC BRANCH EXCHANGE
PC - PERSONAL COMPUTER (HMI WORKSTATION)
PLC - PROGRAMMABLE LOGIC CONTROLLER
PR - PRINTER
RF - RADIO FREQUENCY

INCLUDED SYSTEMS

- SUBSURFACE EMPLACEMENT TRANSPORTATION SYSTEM (FIGURE 5)
- SUBSURFACE ELECTRICAL DISTRIBUTION SYSTEM (FIGURE 16)
- SUBSURFACE VENTILATION SYSTEM (FIGURE 11. 12)
- SUBSURFACE UTILITIES (FIGURE 17)
- SUBSURFACE EXCAVATION SYSTEM (FIGURE 18)
- MUCK HANDLING SYSTEM (FIGURE 18)
- GROUND CONTROL SYSTEM (FIGURE 18)
- PERFORMANCE CONFIRMATION DATA ACQUISITION/ MONITORING SYSTEM (FIGURE 7)

t:#repss#csys#fig#sscs0116.fig

FIGURE 20
SUBSURFACE REP INT CONTROL SYS
PHYSICAL ARCH DIAG - SHT 2



INCLUDED SYSTEMS
- SUBSURFACE RADIOLOGICAL MONITORING SYSTEM (FIGURE 13)
- SUBSURFACE AIR MONITORING SYSTEM (FIGURE 13)

INCLUDED SYSTEMS
- SUBSURFACE FIRE PROTECTION SYSTEM (FIGURE 14)

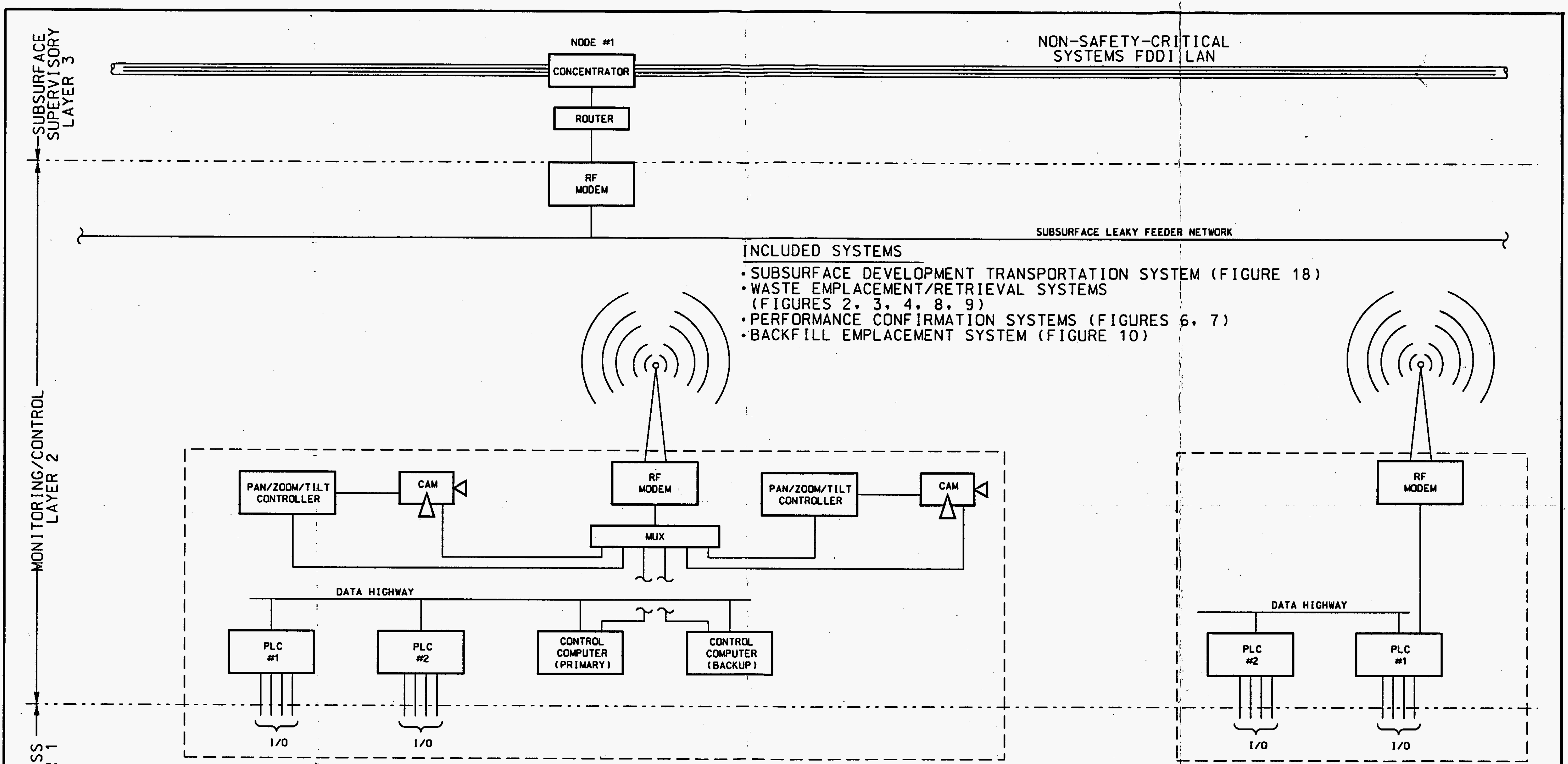
LEGEND:

DCS - DISTRIBUTED CONTROL SYSTEM
I/O - INPUT/OUTPUT
MON - VIDEO MONITOR
MUX - MULTIPLEXER
PA - PUBLIC ADDRESS
PABX - PRIVATE AUTOMATIC BRANCH EXCHANGE
PC - PERSONAL COMPUTER (HMI WORKSTATION)
PLC - PROGRAMMABLE LOGIC CONTROLLER
PR - PRINTER
RF - RADIO FREQUENCY

t:*repss*csys*fig*sscs0117.fig

FIGURE 21
SUBSURFACE REP INT CONTROL SYS
PHYSICAL ARCH DIAG - SHT 3

FILE NAME: W03969/CSYS/FIG/SSCS0117.FIG PD: 8/31/99



INCLUDED SYSTEMS

- SUBSURFACE DEVELOPMENT TRANSPORTATION SYSTEM (FIGURE 18)
- WASTE EMPLACEMENT/RETRIEVAL SYSTEMS (FIGURES 2, 3, 4, 8, 9)
- PERFORMANCE CONFIRMATION SYSTEMS (FIGURES 6, 7)
- BACKFILL EMPLACEMENT SYSTEM (FIGURE 10)

INCLUDED EQUIPMENT

- EMPLACEMENT GANTRY
- REMOTELY OPERATED INSPECTION GANTRY

INCLUDED EQUIPMENT

- WASTE PACKAGE TRANSPORTER
- TRANSPORT LOCOMOTIVE
- EMPLACEMENT GANTRY CARRIER

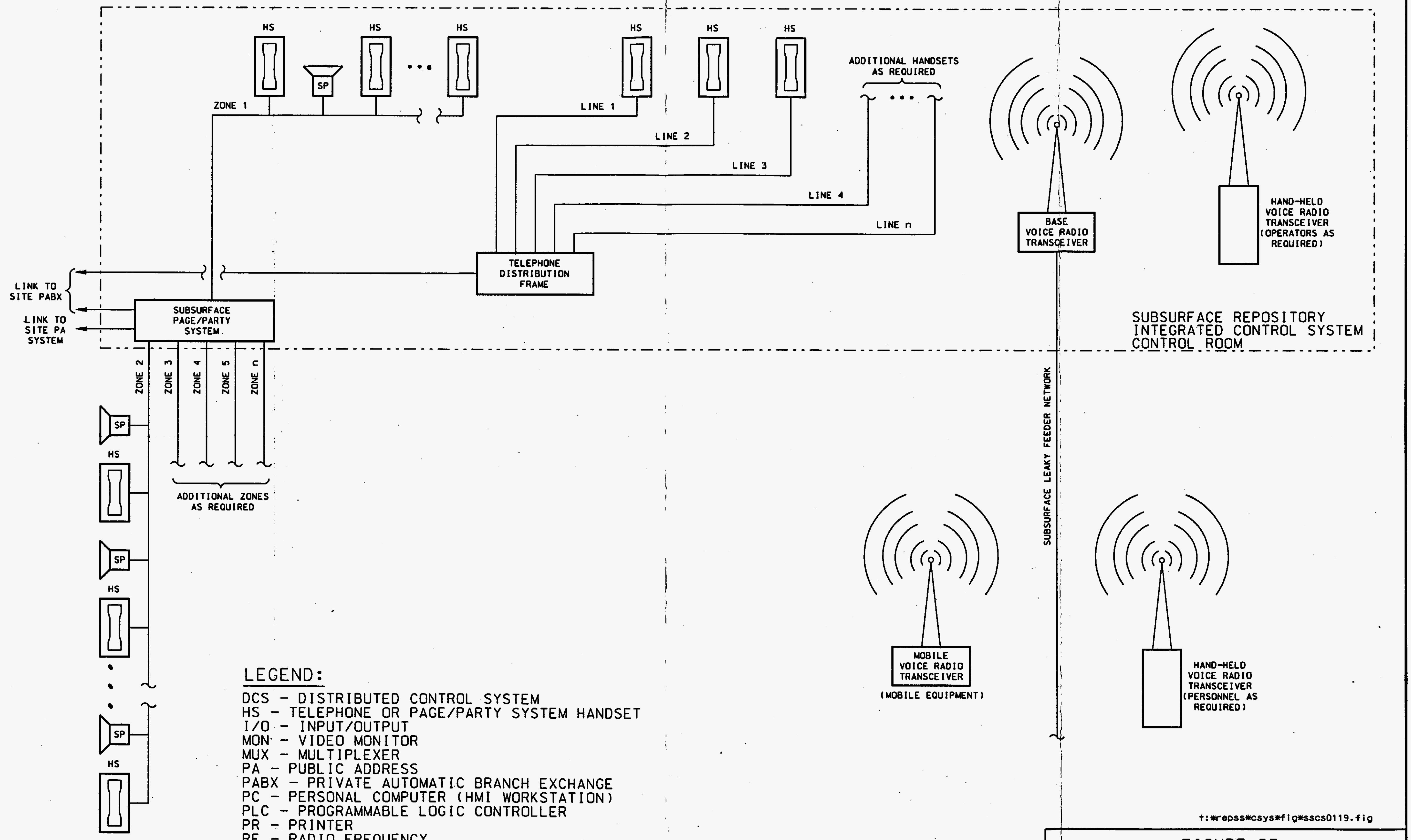
LEGEND:

CAM - VIDEO CAMERA
DCS - DISTRIBUTED CONTROL SYSTEM
I/O - INPUT/OUTPUT
MON - VIDEO MONITOR
MUX - MULTIPLEXER
PA - PUBLIC ADDRESS
PABX - PRIVATE AUTOMATIC BRANCH EXCHANGE
PC - PERSONAL COMPUTER (HMI WORKSTATION)
PLC - PROGRAMMABLE LOGIC CONTROLLER
PR - PRINTER
RF - RADIO FREQUENCY

t:*repss*csys*fig*sscs0118.fig

FIGURE 22
SUBSURFACE REP INT CONTROL SYS
PHYSICAL ARCH DIAG - SHT 4

FILE NAME: W03969/CSYS/FIG/SSCS0118.FIG PD: 09/27/99


HS
SP
HS
HS
HS
HS
HS
ZONE 1
LINE 1
LINE 2
LINE 3
LINE 4
LINE n
ADDITIONAL HANDSETS AS REQUIRED
TELEPHONE DISTRIBUTION FRAME
LINK TO SITE PABX
LINK TO SITE PA SYSTEM
SUBSURFACE PAGE/PARTY SYSTEM
ZONE 2
ZONE 3
ZONE 4
ZONE 5
ZONE n
ADDITIONAL ZONES AS REQUIRED
SP
HS
SP
HS
SP
HS
BASE VOICE RADIO TRANSCEIVER
HAND-HELD VOICE RADIO TRANSCEIVER (OPERATORS AS REQUIRED)
SUBSURFACE REPOSITORY INTEGRATED CONTROL SYSTEM CONTROL ROOM
SUBSURFACE LEAKY FEEDER NETWORK
MOBILE VOICE RADIO TRANSCEIVER
(MOBILE EQUIPMENT)
HAND-HELD VOICE RADIO TRANSCEIVER (PERSONNEL AS REQUIRED)

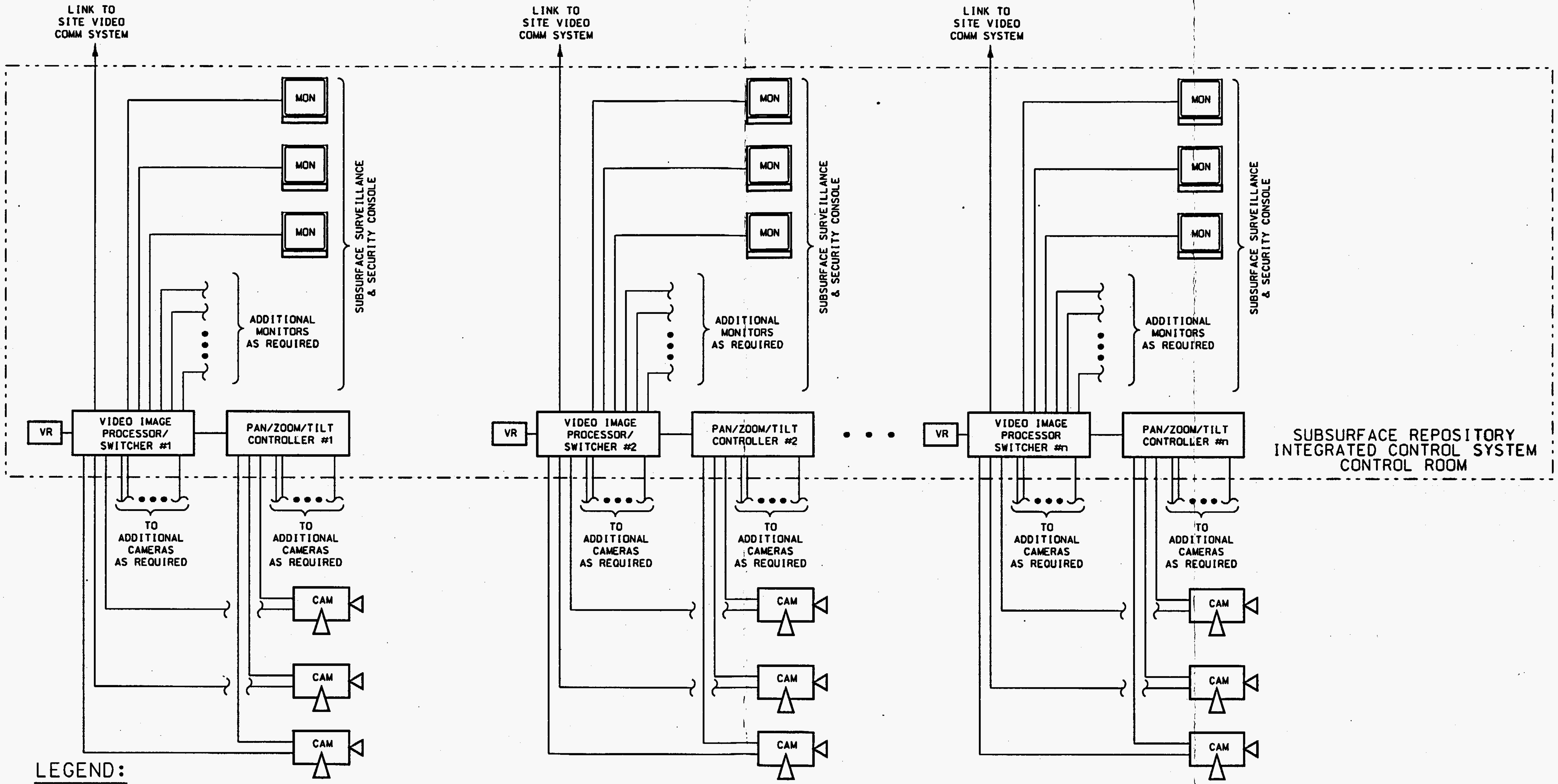
LEGEND:

DCS - DISTRIBUTED CONTROL SYSTEM
HS - TELEPHONE OR PAGE/PARTY SYSTEM HANDSET
I/O - INPUT/OUTPUT
MON - VIDEO MONITOR
MUX - MULTIPLEXER
PA - PUBLIC ADDRESS
PABX - PRIVATE AUTOMATIC BRANCH EXCHANGE
PC - PERSONAL COMPUTER (HMI WORKSTATION)
PLC - PROGRAMMABLE LOGIC CONTROLLER
PR - PRINTER
RF - RADIO FREQUENCY
SP - PAGE/PARTY AREA LOUDSPEAKER

t:*repss*csys*fig*sscs0119.fig

FIGURE 23
SUBSURFACE REP INT CONTROL SYS
PHYSICAL ARCH DIAG - SHT 5

FILE NAME: W03969/CSYS/FIG/SSCS0119.FIG PD: 09/27/99



LEGEND:

CAM - VIDEO CAMERA
DCS - DISTRIBUTED CONTROL SYSTEM
I/O - INPUT/OUTPUT
MON - VIDEO MONITOR
MUX - MULTIPLEXER
PA - PUBLIC ADDRESS
PABX - PRIVATE AUTOMATIC BRANCH EXCHANGE
PC - PERSONAL COMPUTER (HMI WORKSTATION)
PLC - PROGRAMMABLE LOGIC CONTROLLER
PR - PRINTER
RF - RADIO FREQUENCY
VR - VIDEO RECORDER

t:*repss*csys*fig*sscs0120.fig

FIGURE 24
SUBSURFACE REP INT CONTROL SYS
PHYSICAL ARCH DIAG - SHT 6

FILE NAME: W03969/CSYS/FIG/SSCS0120.FIG PD: 09/27/99

## 6.4 SUBSURFACE REPOSITORY INTEGRATED CONTROL SYSTEM DATA COMMUNICATIONS

This section looks at the data communication networks for the subsurface repository facility. In Section 6.2, Subsurface Repository Control System Functional Architecture, functional block diagrams for subsurface control functions are presented based on the primary functions given by the SDDs. In Section 6.3, the physical architecture control and communications equipment for the Subsurface Repository Integrated Control System are grouped in a systematic order to fit the repository layout and its functionality, establishing the integrated control system hierarchy according to the functional roles of the various devices. In this section, a data communications design for the subsurface repository is introduced. This data communications network links the process devices, controllers, control computers, and supervisory workstations together and connects them with other computer and data communications networks. Data communications in a control system play a major role not only in getting information to and from human operators, but also in providing commands and signals that are required for process systems to function. Also, the reliability and safe operation of the integrated control system relies on the integrity of the data communications network.

### 6.4.1 Data Communications Terminology

The following specialty terms and acronyms are used throughout the following subsections describing the data communications system for the subsurface repository:

| | |
|---|---|
| backbone | A network that links a number of LANs together. |
| bridge | A specialized device for inter-networking LANs (linking different LANs together) of the same type (e.g., Ethernet-to-Ethernet). |
| concentrator | A device with multiple ports into which FDDI nodes connect. |
| Ethernet | The most widely used LAN technology. Standard Ethernet runs at 10 Mbps, Fast Ethernet runs at 100 Mbps, and Gigabit Ethernet runs at 1,000 Mbps. |
| FDDI | An acronym for "fiber distributed data interface." A token-passing (see below) LAN technology that runs at 100 Mbps over fiber optic cable configured in a ring topology. |
| hub | The central connection point for wiring an Ethernet LAN. All stations on an Ethernet LAN are linked to each other through the hub. |
| LAN | An acronym for "local area network." A high-speed communications system designed to link computers and other data processing devices together within a small geographic area. |

leaky feeder

A leaky feeder is a radio-based voice and data communication system that utilizes a dedicated signal transmission cable. The systems consists of a number of unidirectional radio frequency bands carried on a repeater network. The coaxial cable comprising the network allows only selected radio signals to "leak" from and to the cable.

modem

A contraction for "MODulation/DEModulation." A device that converts a digital signal to an analog signal for transmission across a network, then converts analog to digital upon reception.

node

An active device on a network.

ring topology

A network whose nodes are connected in a continuous loop.

router

A specialized device for inter-networking LANs (linking different LANs together) of different types (e.g., Ethernet-to-FDDI).

server

A computer that distributes data and provides various network services to a number of devices on a network. These attached devices may be other computers, printers, data communications devices, etc.

star topology

A network whose nodes are connected via point-to-point circuits to the central or hub node.

switch

A hub with basic routing capabilities that connects multiple LANs, either of the same or disparate architectures. It manages traffic on the network by directing incoming packets of data to only those nodes addressed by the packets.

token passing

The transmission of a digital signal consisting of a specific bit pattern across a network by a centralized master control station, indicating the status of the network as available or unavailable. The station in possession of the token is in control of access to the network.

### 6.4.2 Introduction to the Data Communications Design

A preliminary conceptual design for the data communications network for the Subsurface Repository Integrated Control System is presented in Figure 25. While specific types of communications equipment are shown on the diagram, the final decisions concerning the exact nature of these devices will necessarily depend upon further definition of the MGR design as well as evolutionary trends among hardware and software products within the data communications industries. Thus, it is understood that the data communication technologies and protocols offered by this diagram are subject to change or refinement.

The network structures shown in Figure 25 collectively represent the overall physical architecture system (shown in Figures 19 through 22) that combines the controls for the various subsurface process systems into the Subsurface Repository Integrated Control System. The subsurface repository data communications network basically consists of two FDDI ring backbone LANs linked together in a redundant manner—one link at each of two separate nodes. One FDDI backbone is a single-ring network (one cable, two fibers) made up of a number of nodes that link area-specific Ethernet LANs, which, in turn, are connected to those subsurface process systems that this analysis considers to be of a non-critical nature with respect to safety. The other FDDI backbone is a dual-ring network (two cables, two fibers per cable) comprising a number of distributed nodes linking area-specific Ethernet and specialty LANs, which, in turn, are connected to subsurface processes regarded as critical to safety by this analysis. The number of nodes on each FDDI LAN, as well as the number of devices attached to each node, will depend upon the required physical distribution of process monitoring and control equipment throughout the subsurface.

It is important to note in Figure 25 that the Ethernet LAN (along with its attached devices) that is connected to Node #5 of each FDDI LAN is representative of similar equipment connected at FDDI Nodes #2, #3, and #4, and at Nodes #6 through *n*. Furthermore, the various subsurface process systems associated with each Ethernet LAN, and listed under Node #5 of each FDDI LAN, are also typical for each of the other FDDI nodes mentioned previously. The non-safety-critical systems FDDI LAN includes the Subsurface Emplacement Transportation System, the Subsurface Electrical Distribution System, the Subsurface Ventilation System, the Subsurface Water Distribution System, the Subsurface Water Collection System, the Subsurface Compressed Air System, the Subsurface Excavation System, the Muck Handling System, and the Ground Control System. The safety-critical systems FDDI LAN includes the Subsurface Fire Protection System, the Subsurface Radiological Monitoring System, and the Subsurface Air Monitoring System.

The subsurface leaky feeder network shown connected to Node #1 of the non-safety-critical systems FDDI LAN is unique to that same node. This is also true of the various subsurface process systems associated with this leaky feeder network. These systems include the Waste Emplacement System, the Waste Retrieval System, the Subsurface Development Transportation System, the Performance Confirmation Emplacement Drift Monitoring System, the Performance Confirmation Data Acquisition/Monitoring System, the Performance Confirmation Emplacement Drift Monitoring System, and the Backfill Emplacement System. Finally, the LAN and supervisory computer equipment shown residing within the control room for the Subsurface Repository Integrated Control System is unique to Node #1 of each FDDI LAN.

### 6.4.3 Data Communications Design

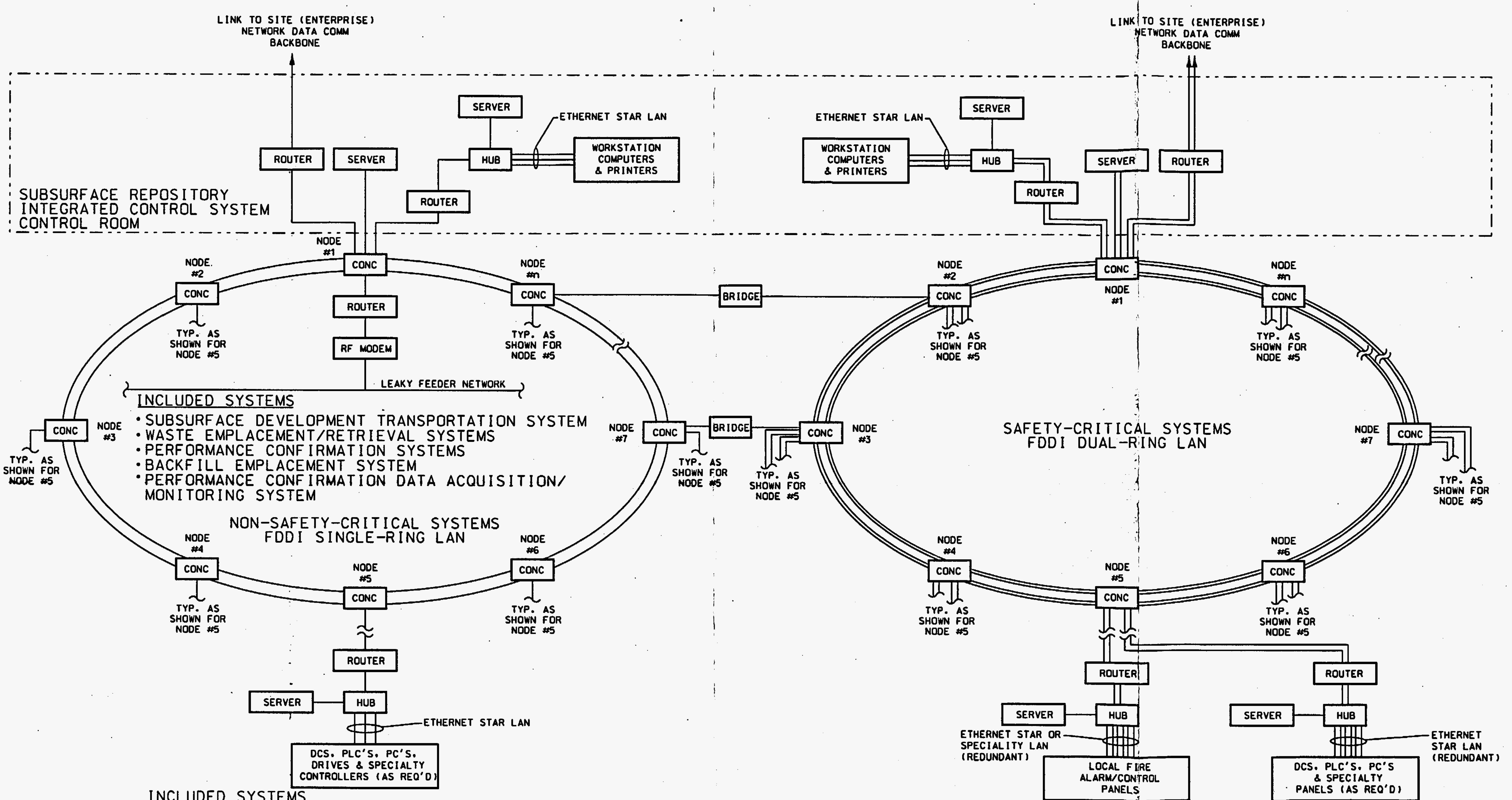
As mentioned earlier, the subsurface data communications system consists of two FDDI ring backbone LANs linked together in a redundant manner, one configured as a single ring for non-safety-critical data and the other configured as a dual ring for safety-critical data. The single ring uses two fiber optic strands, each transmitting the same data in opposite directions at the same time. This gives the ring the ability to heal itself in the event of a cable break at some point on the ring. The two rings in a dual-ring configuration each work as a single ring. Like the first ring, the second ring consists of two fiber optic strands usually contained within a separate cable, and is simply used as a backup to the first in the event of a major communication failure. A dual ring operates in a dual counter-rotating manner. This means that they transmit the same data in opposite directions simultaneously. That is, the counter-rotating design ensures that all nodes attached to the rings will not be cut off from network services regardless of the location of the cable failure. Furthermore, the dual counter-rotating design allows the ring to wrap itself around any failed node on the ring. Also, by using concentrators at node locations, multiple nodes may fail without disrupting ring integrity. The two FDDI rings are linked together at two separate nodes in order to effect a redundant data path between the two backbone networks. The reason for this link is information sharing between the safety-critical and non-safety-critical systems, primarily for the purpose of providing control interlocks between the two different classes of systems.

The primary reasons for choosing FDDI-based LANs for the two backbones making up the subsurface data communications system are inherent fault tolerance (due, in part, to the ring configuration), transmission speed, and ability to cover long distances. The fault tolerant characteristics of FDDI LANs were discussed briefly above. The data rate achieved by a typical FDDI ring is one hundred million bits per second (100 Mbps), which is a much higher data rate than standard Ethernet or other data communication technologies such as Token Ring. Although other communication services such as asynchronous transfer mode (ATM) offer data rates of 155 Mbps or better and possess greater bandwidth, FDDI is presently recommended as the data communications backbone for the MGR subsurface primarily because of its current widespread use, strong vendor support, and mature set of standards. On the other hand, ATM is a relatively new and somewhat unproven technology at this time and its future is unclear. Asynchronous transfer mode standards are still maturing and industry is just beginning to gain experience with ATM in production environments. Moreover, ATM solutions have few and somewhat precarious relationships with communications equipment vendors. Because of the use of fiber optic cable inherent in FDDI design, FDDI rings span greater distances than its wire-based counterparts. The total maximum ring length for a FDDI ring is one hundred kilometers (100 km) and the maximum distance between nodes is two kilometers (2 km). The FDDI rings also allow a maximum number of one thousand attached nodes.

Most of the individual nodes attached to the two FDDI ring backbones are each linked to an Ethernet LAN configured in a star topology. That is, the different devices on each Ethernet LAN are each connected to an intelligent central wiring hub by an individual segment of fiber optic cable. Through the use of intelligent hubs, Ethernet star topologies have been developed that are able to manage data flow and provide deterministic data transmissions. Such hubs provide data buffering and are capable of determining which network segments have devices that want data. As a result, data collisions and, thus, data retransmissions, are minimized. Perhaps the principal advantage of a star topology is that the failure of any individual node on the hub will not affect the remainder of the network. Moreover, it is a relatively simple matter to accommodate new devices or move existing devices from one location to another in a start topology. It is also less difficult to troubleshoot and isolate networking problems on a star LAN than many other topologies. Devices that are star-connected to each of the Ethernet LANs linked to each node of the safety-critical systems FDDI ring have redundant data paths in order to further improve the overall fault tolerance of the safety-critical systems network throughout.

At the present time, Ethernet is primarily used for information networks. However, Ethernet is rapidly emerging as a natural choice for data communications in the process control and automation industries, largely because transmission control protocol/internet protocol, known as TCP/IP, its most popular LAN protocol, is widely supported by most computer and industrial control product manufacturers. Recent innovations in Ethernet technology have improved the deterministic features and performance of Ethernet.

The subsurface leaky feeder network attached to Node #1 of the non-safety-critical systems FDDI ring backbone represents just one of two candidate data communication technologies being considered for the monitoring and control of the transport locomotives and other specialized rail vehicles. The other data communication technology under consideration at this time is slotted microwave. The selection and depiction of a leaky feeder network shown in Figure 25 for the remote control of mobile rail equipment is strictly for illustrative purposes only. Although not shown in Figure 25, the communication links from the FDDI backbone to the other types of networks being considered for this purpose will be similar. The final selection of the actual data communication networks to be employed for the subsurface mobile rail vehicles is beyond the scope of this analysis. Additional details for these different communication technologies and a comparative evaluation are presented in Sections 7.4.2 and 7.4.4 of the *Subsurface Waste Package Handling – Remote Control and Data Communications Analysis* (DIRS 24).



INCLUDED SYSTEMS
- SUBSURFACE DEVELOPMENT TRANSPORTATION SYSTEM
- WASTE EMPLACEMENT/RETRIEVAL SYSTEMS
- PERFORMANCE CONFIRMATION SYSTEMS
- BACKFILL EMPLACEMENT SYSTEM
- PERFORMANCE CONFIRMATION DATA ACQUISITION/ MONITORING SYSTEM

INCLUDED SYSTEMS
- SUBSURFACE EMPLACEMENT TRANSPORTATION SYSTEM
- SUBSURFACE ELECTRICAL DISTRIBUTION SYSTEM
- SUBSURFACE VENTILATION SYSTEMS
- SUBSURFACE UTILITIES
- SUBSURFACE EXCAVATION SYSTEM
- MUCK HANDLING SYSTEM
- GROUND CONTROL SYSTEM
- PERFORMANCE CONFIRMATION DATA ACQUISITION/ MONITORING SYSTEM

INCLUDED SYSTEMS
- SUBSURFACE FIRE PROTECTION SYSTEM

INCLUDED SYSTEMS
- SUBSURFACE RADIOLOGICAL MONITORING SYSTEM
- SUBSURFACE AIR MONITORING SYSTEM

LEGEND:

FDDI - FIBER DISTRIBUTION DATA INTERFACE
CONC - CONCENTRATOR
LAN - LOCAL AREA NETWORK
DCS - DISTRIBUTED CONTROL SYSTEM
PLC - PROGRAMMABLE LOGIC CONTROLLER
PC - PERSONAL COMPUTER
RF - RADIO FREQUENCY

t:*repss*csys*fig*sscs0114.fig

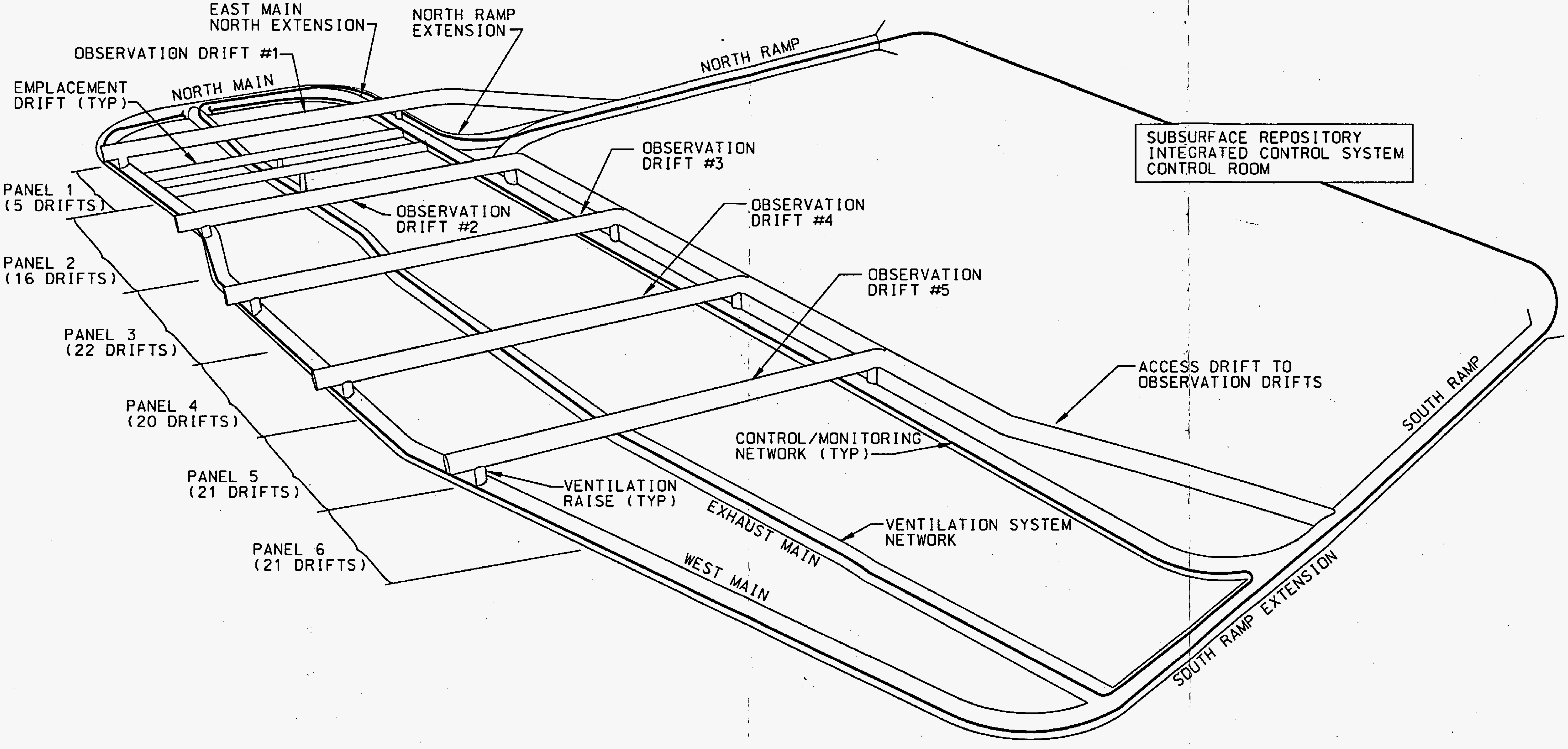
FIGURE 25
SUBSURFACE REP INT CTRL SYS
DATA COMMUNICATIONS NETWORK

FILE NAME: W03969/CSYS/FIG/SSCS0114.FIG PD: 09/27/99

### 6.4.4 Data Communications Cable Layout

Figure 26 shows a preliminary data communications cable layout for the proposed subsurface repository. The cable routing design is conceptual only and is not intended for construction purposes. Both the non-safety-critical and the safety-critical FDDI backbone LANs will follow the same path as shown throughout the underground facility, and at the surface, through the control room for the Subsurface Repository Integrated Control System. As can be seen from the layout, the routing path of these fiber optic cables is unaffected by the different phases of emplacement drift construction and is therefore to be considered a permanent installation.

As shown in Figure 25, the network nodes of each FDDI backbone consist of an Ethernet LAN linked to concentrators. Therefore, data concentrators and other LAN devices will have to be placed in various protected locations throughout the repository.



t:*repss*csys*fig*sscs0122.fig

LEGEND:

━━ FDDI BACKBONE LANS

FIGURE 26
SUBSURFACE DATA COMM NETWORK
CABLE LAYOUT

FILE NAME: WO3969/CSYS/FIG/SSCS0122.FIG PD: 09/27/99

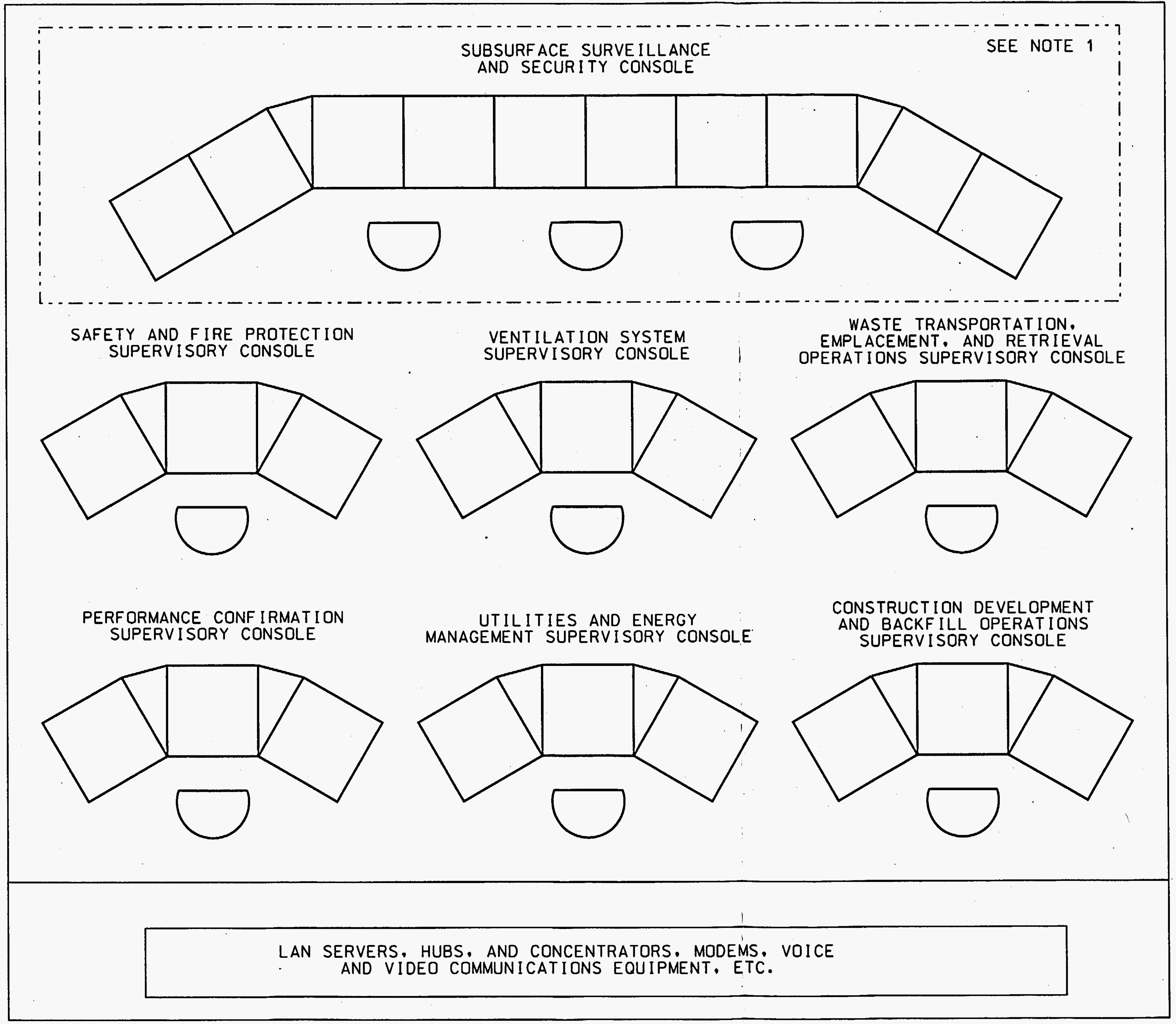
### 6.4.5 Data Communications Summary

The evolving components of computer technology, together with improvements in LAN data management devices, network transmission media (e.g., fiber optics), and developments in integrated data, voice, and video systems, are forcing data communications system manufacturers to introduce new products and related technologies at an unprecedented rate. This exploding growth in technology is rendering today's systems obsolete in just a few years. Because of these rapidly evolving data communication systems technologies, the data communications system design proposed in this document is to be considered preliminary and should not be understood to serve as the definitive solution for the subsurface data communications network. It does, however, reflect much of today's "state of the art" in the data communications industry, and can be used as a starting point for detailed design and the development of documents for cost estimating, planning, etc. It will be necessary to maintain continued surveillance of Nuclear Regulatory Commission requirements and to work closely with major data communications product manufacturers to update the emerging data communications system design if the project schedule and expected license application requirements are to be met.

## 6.5 SUBSURFACE REPOSITORY OPERATIONS CONTROL ROOM DESIGN

Figure 27 presents a preliminary design layout for a control room within the Central Control Center for the subsurface portion of the MGR OMCS, known as the Subsurface Repository Integrated Control System. Subsurface monitoring and/or control functions are conducted by operations personnel from seven supervisory consoles, each consisting of several HMI workstation computers, telephone handsets, video monitors and recorders, and data printers. Generally speaking, each supervisory console is responsible for multiple process systems throughout the subsurface. The systems assigned to each console are described in Section 6.3.4. The number of modular sections that make up each console and the number of chairs/operators shown for each is conceptual only. The actual quantities of the various devices within a given console will be determined by the extent and complexity of the processes monitored and/or controlled from that console. Furthermore, the total number of operators permanently assigned to a given console will be determined by the number of HMI devices and/or video monitors that comprise that console. Also shown in the figure, in an area separate from the subsurface operations floor, is an equipment room containing various data, voice, and video communications equipment not normally accessed by operations personnel.

Each supervisory console for process monitoring and control that is shown in Figure 27 corresponds to each group of devices shown on the subsurface supervisory layer (layer 3) of Figure 19. The subsurface surveillance and security console shown in Figure 27 corresponds to the group of video monitoring and recording equipment shown in Figure 24. This console will probably be located in an area apart from the other consoles, either in the same control room or in another room within the Central Control Center. It is intended that the different types of telephone handsets and portable radio transceivers shown as located in the control room for the Subsurface Repository Integrated Control System (Figure 23) should be distributed as required among the various supervisory consoles of Figure 27. That is, the operator(s) at each console should have a full complement of devices for voice communication at their disposal. It is also intended that a number of video monitors for subsurface operations be similarly distributed among several subsurface process monitoring and control supervisory consoles. For example, the supervisory console for waste transportation, emplacement, and retrieval operations will house video monitors to assist remote operators overseeing or directly controlling these system activities. For similar reasons, video monitors will also be required for the supervisory console for the construction development and backfill operations, and at the supervisory console for performance confirmation.


SUBSURFACE SURVEILLANCE AND SECURITY CONSOLE
SEE NOTE 1
SAFETY AND FIRE PROTECTION SUPERVISORY CONSOLE
VENTILATION SYSTEM SUPERVISORY CONSOLE
WASTE TRANSPORTATION, EMPLACEMENT, AND RETRIEVAL OPERATIONS SUPERVISORY CONSOLE
PERFORMANCE CONFIRMATION SUPERVISORY CONSOLE
UTILITIES AND ENERGY MANAGEMENT SUPERVISORY CONSOLE
CONSTRUCTION DEVELOPMENT AND BACKFILL OPERATIONS SUPERVISORY CONSOLE
LAN SERVERS, HUBS, AND CONCENTRATORS, MODEMS, VOICE AND VIDEO COMMUNICATIONS EQUIPMENT, ETC.

NOTES:

1. EQUIPMENT LOCATED IN A SEPARATE AREA OF CONTROL ROOM OR SEPARATE ROOM IN THE CONTROL CENTER.

t:*repss*csys*fig*sscs0121.fig

FIGURE 27
SUBSURFACE REP INT CONTROL SYS
CONTROL ROOM LAYOUT

FILE NAME: W03969/CSYS/FIG/SSCS0121.FIG PD: 09/27/99

## 6.6 SAFETY STRATEGIES AND REQUIREMENTS

An overview of the pre-closure safety case strategy for the MGR is characterized in the *Monitored Geologic Repository Instrumentation and Control System Strategy* document (DIRS 35).

### 6.6.1 Subsurface Repository Integrated Control System Safety-Related Features

A major role of the Subsurface Repository Integrated Control System is to manage and control a number of safety-critical functions of various processes throughout the subsurface facility. A safety-critical function, for purposes of this analysis, is a function that can have a direct effect on the wellbeing of human life, equipment, or the environment. Therefore, it is important that the design development of the Subsurface Repository Integrated Control System, as well as the various process monitoring/control systems it integrates, proceeds with these safety-related issues in mind. The following items represent general strategic features or design aims of those portions of the Subsurface Repository Integrated Control System intended to perform safety-critical functions.

*Reliability* is the probability of a system or component of a system functioning correctly over a given period of time under a given set of operating conditions. Here “functioning correctly” is taken to mean “operating as defined within its specification.” It is assumed that the component or system was functioning correctly at the beginning of the period in question. Thus, the reliability of a component or system varies with time. Therefore, when reliability issues are being assessed during the design of the Subsurface Repository Integrated Control System, it is very important to consider the performance of the system and its components over an appropriate length of service. Reliability is of particular relevance in portions of the Subsurface Repository Integrated Control System where continuous, uninterrupted operation is essential to safety.

The *availability* of a system is the probability that the system will be functioning correctly at any given time. Like reliability, the availability of a system varies with time. However, unlike reliability, the availability of a system relates to a particular point in time rather than to a given period. Availability is of great importance in portions of the Subsurface Repository Integrated Control System and various local process control systems that are not used continuously.

A *fail-safe operation* refers to a set of output states of a system that can be identified as being safe. The Subsurface Repository Integrated Control System, as well as the various process monitoring/control systems it integrates, should be designed to “fail safe” by ensuring that it adopts these outputs in the event of failure or the inability to recover from failure.

*System integrity* refers to the ability of a system to detect faults in its own operation and to inform a human operator of such faults. System integrity is of particular importance in systems that possess fail-safe states. This is because it is desirable that a system be designed so that it will enter the fail-safe state if there is any uncertainty about the correctness of the system’s performance.

*Data integrity* is the ability of a system to prevent damage to its own database and to detect, and possibly correct, errors that do occur. Data integrity will be of importance in the Subsurface

Repository Integrated Control System where data used by certain portions of the system are deduced and stored rather than measured directly.

*System recovery* refers to the ability of a system to restart and return to its normal state of operations after failure due to a fault. Depending on the nature of the process operations involved, the recovery process of the Subsurface Repository Integrated Control System, along with the various process monitoring/control systems it integrates, may need to determine current process status and take appropriate action to continue operation to maintain safety.

The *maintainability* of a system is its ability to be retained in or returned to its designed operating state. The maintenance of portions of the Subsurface Repository Integrated Control System and portions of local process systems related to safety is greatly affected by the type of process being monitored/controlled. In some cases, maintenance may be performed while the system is in service. This may entail performing repairs or preventative maintenance on a running system, or shutting it down temporarily. Alternatively, maintenance may only be possible between periods of service.

*Dependability* is a property of a system that justifies the reliance placed on it. Dependability, quantified in terms of a number of the above features such as reliability and availability, combine to produce a dependable system.

In addition to incorporating the design strategies discussed above, the Subsurface Repository Integrated Control System will have to satisfy certain specific safety requirements relating to its functions and characteristics in order to be able to properly control safety-related operations. A series of tasks must be performed to determine these system-specific requirements. The main stages of this process may be categorized as follows:

- Identification of the hazards associated with the system
- Classification of these hazards
- Determination of methods for dealing with the hazards
- Assignment of appropriate reliability and availability requirements

To determine the characteristics that a system must have in order to be safe, it is necessary to understand the ways in which the system could harm persons, equipment, or the environment. A *hazard* is the capacity of a system to do harm to people, property, or the environment. As such, the formal task of hazard analysis should be undertaken in order to identify potential hazards associated with a given system.

Having identified the hazards associated with a system, it is useful to classify them by severity and nature. The severity of a hazard is related to the consequences of any accident that might occur as a result of that hazard. The importance of a hazard is related to both its severity and frequency of occurrence. These two factors combine within the concept of *risk*. This suggests that a formal risk analysis needs to be performed to determine the classification and acceptability of the risk associated with a given hazard.

Having identified all the hazards within a system, it is then necessary to identify methods for dealing with each of them. For each operation that a system can perform, it is necessary to decide the conditions for which that operation is safe. Once appropriate conditions for safety have been established, these then become part of the formal safety requirements of the system. The safety requirements of a system provide the basis for assigning reliability and availability requirements to the system. This is an assessment process that is accomplished through formal reliability modeling techniques.

As a necessary part of the design for the Subsurface Repository Integrated Control System, it is recommended that the above tasks be topics for future analyses and models.

### 6.6.2 Safety-Related Requirements for Computer-Based Control Systems

As stated in the previous subsection, a major role of the Subsurface Repository Integrated Control System is to manage and control a number of safety-critical functions of various processes throughout the subsurface facility. Since the Subsurface Repository Integrated Control System is based on digital computer technology, it follows that a number of integral components of various safety-critical systems used throughout the subsurface repository for process monitoring and control are computer-based devices. Furthermore, since the monitoring and control of these systems takes place in a nuclear environment, it would be sound practice to examine the standards and regulations governing the use of digital computers in the safety systems of commercial nuclear power plants to determine the computer-specific requirements of the Subsurface Repository Integrated Control System at Yucca Mountain. Therefore, it is recommended that IEEE Standard 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations" (DIRS 40) and IEEE Standard 7-4.3.2-1993, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations" (DIRS 37) (See Section 4.3.2 herein) be consulted to establish the functional and design requirements for the computer-based components of the Subsurface Repository Integrated Control System. These two standards have been endorsed by the U.S. Nuclear Regulatory Commission in Regulatory Guide 1.152, "Criteria for Digital Computers in Safety Systems of Nuclear Power Plants" (DIRS 63) and Regulatory Guide 1.153, "Criteria for Safety Systems" (DIRS 64), respectively (Section 4.3.3).

The items listed below represent a number of safety system criteria cited within the two IEEE standards from which computer-specific requirements were developed for nuclear power generating stations.

#### 6.6.2.1 Single-Failure

A single-failure analysis shall be performed. A single-failure analysis verifies that no single failure in either the hardware or software of the computer will cause failure in channels or actuation circuits that would cause the loss of a safety function. The single-failure analysis shall be performed in conjunction with a comprehensive facility analysis of the MGR.

#### 6.6.2.2 Completion of Protective Action

The system logic for the safety systems shall be designed such that once initiated automatically or manually, the intended sequence of protective actions of the execute features shall continue until completion. Deliberate operator action shall be required to return the safety system to normal.

#### 6.6.2.3 Quality

Computer hardware components shall be of a quality that is consistent with minimum maintenance requirements and low failure rates, and shall be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program, consistent with the requirements of ASME NQA-1-1997, "Quality Assurance Program Requirements for Nuclear Facility Applications" (DIRS 36) (see Section 4.3.1).

Computer software components shall be developed, modified, or accepted in accordance with an approved software quality assurance plan, consistent with the requirements of ASME NQA-1-1997, "Quality Assurance Requirements for Nuclear Facility Applications" (DIRS 36). Guidance for developing a software quality assurance plan may be found in IEEE Standard 730-1998, "IEEE Standard for Software Quality Assurance Plans" (DIRS 41) and IEEE Standard 730.1-1995, "IEEE Guide for Software Quality Assurance Planning" (DIRS 42) (Section 4.3.2).

The qualification process for commercially available computer hardware and software shall entail identification of functional and performance requirements necessary to provide adequate confidence that the safety functions can be achieved. In addition, the qualification process for hardware and software shall, wherever practicable, include an evaluation of the design process.

Verification and validation shall be performed for the development and modification of computer software in accordance with IEEE Standard 1012-1986, "IEEE Standard for Software Verification and Validation Plans" (DIRS 47) (Section 4.3.2). This standard has been endorsed by the U.S. Nuclear Regulatory Commission Regulatory Guide 1.168, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (DIRS 65) (Section 4.3.3).

Computer software configuration management shall be performed in accordance with a software configuration management plan. Guidance for the development of a software configuration management plan may be found in IEEE Standard 828-1990, "IEEE Standard for Software Configuration Management Plans" (DIRS 43) and ANSI/IEEE Standard 1042-1987, "IEEE Guide to Software Configuration Management" (DIRS 51) (Section 4.3.2). These standards have been endorsed by the U.S. Regulatory Commission Regulatory Guide 1.169, "Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants" (DIRS 66) (Section 4.3.3).

#### 6.6.2.4 Equipment Qualification

Equipment qualification testing shall be performed with the computer functioning with computer software and diagnostics that are representative of those used in actual operation. All portions of the computer necessary to accomplish a safety function, or those portions whose operation or failure could impair the safety function, shall be exercised during testing.

#### 6.6.2.5 System Integrity

The computer shall be designed to perform the safety function when subjected to any condition, external or internal, that has a significant potential for defeating the safety function.

The test and calibration function shall not adversely affect the ability of the computer to perform its safety functions.

#### 6.6.2.6 Independence

Barrier requirements shall be identified to provide adequate confidence that the non-safety portions cannot interface with performance of the safety portion of the computer software.

#### 6.6.2.7 Capability for Test and Calibration

Capability for testing and calibration of safety system equipment shall be provided while retaining the capability of the safety systems to accomplish their safety functions.

#### 6.6.2.8 Information Displays

Display instrumentation shall provide accurate, complete, and timely information pertinent to safety system status.

If the protective actions of some part of a safety system have been bypassed or deliberately rendered inoperative for any purpose other than an operating bypass, continued indication of this fact for each affected safety group shall be provided in the control room.

#### 6.6.2.9 Control of Access

The design shall permit the administrative control access to safety system equipment.

#### 6.6.2.10 Repair

The safety system shall be designed to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment.

#### 6.6.2.11 Auxiliary Features

Auxiliary supporting features that (1) perform a function that is not required for the safety systems to accomplish their safety function, and (2) are part of the safety systems by association shall be designed to meet those criteria necessary to ensure that these components, equipment, and systems do not degrade the safety systems below an acceptable level.

#### 6.6.2.12 Human Factors Considerations

Human factors shall be considered at the initial stages and throughout the MGR OMCS design to assure that the functions allocated in whole or in part to the human operator(s) and maintainer(s) can be successfully accomplished to meet the safety system design goals, in accordance with IEEE Standard 1023-1988, "IEEE Guide for the Application of Human Factors Engineering to

Systems, Equipment, and Facilities of Nuclear Power Generating Stations" (DIRS 49) (Section 4.3.2).

#### 6.6.2.13 Reliability

An appropriate reliability analysis of the design shall be performed in order to confirm that quantitative and qualitative reliability goals have been achieved. Guidance for the development of a reliability analysis may be found in IEEE Standard 352-1987, "IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Protection Systems" (DIRS 38) and IEEE Standard 577-1976, "IEEE Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Power Generating Stations" (DIRS 39) (Section 4.3.2).

## 6.7 OFF-NORMAL EVENTS AND RESPONSES

### 6.7.1 Off-Normal Events and the Subsurface Repository Integrated Control System

An off-normal event, as discussed in this analysis, is any occurrence or activity in subsurface repository operations that is either unexpected or different from what would otherwise be considered as part of normal operations, but is not as catastrophic as a design basis event. The Safety Analysis Group within the Repository Systems Operation organization has the primary responsibility for identifying design basis events and then analyzing each of them for the potential magnitude of their effect on the MGR. Based on the results of these analyses, design considerations will be communicated to other design organizations. Consequently, a discussion regarding design basis events will not be undertaken in this analysis. Design basis events are briefly discussed in the *Monitored Geologic Repository Instrumentation and Control System Strategy* document (DIRS 35).

Subsurface off-normal events would include incidents such as electrical power losses, electrical power dips and surges, equipment and component failures, etc. How these types of events are recognized and handled is an important aspect of the Subsurface Repository Integrated Control System. Therefore, it is imperative that the impact and consequences of such events on subsurface repository operations be examined to ensure that they can be responded to in a safe and timely manner by the subsurface controls. Specifically, the Subsurface Repository Integrated Control System must have the necessary features to ensure an organized and planned response to off-normal events. The discussion in this section will assist in laying out a foundation for addressing off-normal events that will serve as a basis for further development by subsequent analyses. Operator response to off-normal events noted above will be developed in an emergency or alarm response system procedure.

### 6.7.2 Responses to Off-Normal Events

As a minimum, the major responses to an off-normal event by the Subsurface Repository Integrated Control System are:

- Minimize or prevent, to the greatest extent possible, disruptions to unaffected operations.

- Shutdown and secure the necessary or required on-going processes in the proper order and in a timely manner.

In an effort to achieve these two responses, the Subsurface Repository Integrated Control System design will need to incorporate the planned response(s) to each off-normal event. Control system responses will affect the reliability, availability, and maintainability requirements of the Subsurface Repository Integrated Control System. For example, a defense-in-depth design would include features such as redundancy, independence, and diversity, which would play a significant role in assuring the reliability and availability of control system responses. Clearly, strategic features such as these are intimately related to the idea of risk with respect to the control of subsurface operations. Performing a risk assessment study for each identifiable off-normal event will greatly assist in determining the response requirements for each event. Depending on the number of risk factors associated with an off-normal event, the degree of stringency of the control system design criteria will be proportional to those risk factors.

### 6.7.3 Responses to Off-Normal Events

The manner in which the Subsurface Repository Integrated Control System handles and responds to off-normal events, while continuing its normal control operations for unaffected processes, is of utmost importance in the design development of this system. As a minimum, the design development phase should consider the following as means for effecting responses to various off-normal events:

- General alarm and personnel notification systems
- Emergency shutdowns
- Emergency response plans
- Manual overrides
- Backup power supplies

Careful consideration will have to be given to the selection and location of alarm and personnel warning devices that would typically operate under off-normal conditions. Moreover, determining not only which personnel and interfacing systems need to be notified of an off-normal event, but also how they are to be notified, is essential to maintain the operational integrity, safety, and security of the entire MGR site.

A response to an off-normal event that requires an emergency shutdown of some system or piece of equipment may include an orderly and safe shutdown of related but separate equipment and systems. A determination will need to be made as to which systems need to be shutdown and in what order for the off-normal event(s) taking place. It is quite likely that a combination of both manual and automatic actions will carry out these shutdown operations. The process of determining what combinations of these actions are both safe and appropriate in response to the event(s) will involve further study and analysis. A related yet separate determination will need to be made as to both the means (manual or automatic) as well as the sequential order for restarting or recovering these same systems. This determination will also involve further study and analysis.

Responses to off-normal events may have significant effects on the emergency response plans for the MGR site, particularly those plans governing the subsurface portion of the facility. It remains to be determined exactly how and to what extent the responses of the Subsurface Repository Integrated Control System to off-normal events will impact the various plans and procedures that comprise the emergency response system of the MGR.

Manual overrides will be a necessary means for responding to certain types of off-normal events. The Subsurface Repository Integrated Control System will need to provide for manual control of certain equipment and systems that must continue to operate in the event of automatic controls failure. The control system must also provide for the manual override of automatic controls for certain processes or initiate specific emergency responses to system failures. A major consideration here is the design of the interface between the human operator and the process affected by the off-normal condition.

An uninterruptible power supply represents a complete and total response solution to the problem of an off-normal event that results from a loss of primary electrical power to some process equipment item or system. However, numerous constraints on the subsurface emergency power distribution system will no doubt prohibit a tie-in for each and every electrical equipment item and system. Therefore, only a few select equipment items and systems (including control systems) throughout the subsurface facility will likely have this backup power capability. The determination as to which systems will carry this feature will become an increasingly important issue as the control system design progresses for the subsurface facility.

### 6.7.4 Off-Normal Events and Responses Summary

The conceptual design for the Subsurface Repository Integrated Control System presented elsewhere in this analysis will be able to accommodate and support the design criteria and features required for responding to off-normal events.

Several general procedures are recommended for approaching the design development of control system responses to off-normal events. Of paramount importance is that all design aspects of the Subsurface Repository Integrated Control System be thoroughly investigated and reviewed in accordance with these procedures for impacts from off-normal events. These procedures include, as a minimum:

- Identify and review the various I&C systems that are affected by off-normal events.
- Investigate and formulate I&C system requirements for responding to off-normal events.
- Consider personnel and public safety to be the overriding concern in defining responses to off-normal events.

The ideas presented and discussed in this section merely identify issues and guidelines in connection with the treatment of off-normal events by the Subsurface Repository Integrated

Control System. As such, further investigation and refinement of these ideas and others as they are identified is in order and hence, should be the subject task of a future analysis.

## 6.8 SOFTWARE DEVELOPMENT STRATEGIES

Software planning and development for process control and communications represents major issues with respect to system design. In particular, software planning and development for the Subsurface Repository Integrated Control System will be a significant work activity in terms of both time and cost for the Project. A large number of different types of software development packages will likely be used to develop running programs for the various computer-based components of the system for process monitoring and control, as well as for data, voice, and video communications. Most of these various software development products will likely be available as commercial off-the-shelf development packages and tools from which most of the running application programs for the system will be created. However, it is expected that some of the system computer programs will have to be developed using low-level programming techniques, without the benefit of any commercially available application development platform. The need for such an approach would probably be due, at least in part, to the use of specialized hardware components within the system. Therefore, it is anticipated that an extensive and complex software configuration and programming effort will be required to achieve fully reliable and efficient control and communications software programs for the Subsurface Repository Integrated Control System.

### 6.8.1 Software Planning and Development Program

A software planning and development program for the Subsurface Repository Integrated Control System is presented as a set of numbered work package activities and their descriptions in the *Repository Subsurface Control Integration Plan* (refer to DIRS 34, Attachment II, Activities 31 through 41). Taken collectively, these activities address a number of software-related design issues, such as programming methodologies, program approach and planning, quality controls and assurances, regulatory approval strategies, implementation and testing, life-cycle operations, verification and validation, and program technical support and maintenance. These issues will demand time and attention throughout the design, implementation, and startup phases of the Subsurface Repository Integrated Control System.

In addition to the work activities referenced above that comprise the software planning and development program, the program may contain a number of other items that affect software planning and development. For example, the program may contain a general statement that gives an overview and philosophy (rationale) of the planning and development strategy. A statement describing the policy requirements for high-level project software may also be included. The program may also define software life-cycle terms, development phases and success criteria, milestone review criteria, specifications and review criteria of software end products, and the organization/division of responsibilities among members of the development team. Of these items, perhaps one of the most fundamental is specification of the software development phases and the milestone reviews associated with each.

The following table provides a chronological list of development phases and milestone reviews that could be used to model the software life-cycle process for the Subsurface Repository Integrated Control System.

Table 3. Software Life-Cycle Phases and Milestone Reviews

| Order | Phases | Milestone Reviews |
|---|---|---|
| 1 | System Requirements Analysis | • System Functional Requirements<br>• System Management Plan |
| 2 | System Functional Design | • System Functional Design<br>• Subsystem Work Implementation Plan |
| 3 | Subsystem Requirements Analysis | • Software Requirements |
| 4 | Subsystem Functional Design | • Subsystem Functional Design<br>• Software Work Implementation Plan |
| 5 | Software Requirements Analysis | • Software Requirements |
| 6 | Software Design | • Software Design |
| 7 | Software Implementation and Test | • Implementation Status<br>• Software Delivery |
| 8 | Subsystem Integration, Test, and Delivery | • Subsystem Delivery |
| 9 | System Implementation, Test, and Delivery | • System Delivery |
| 10 | Operation and Maintenance | --- |

Software planning and development within the context of safety-critical systems takes on an added dimension in terms of strategic features and requirements. A detailed discussion of software planning and development for the control of safety-critical systems is presented in Section 6.6.2.

### 6.8.2 Software Types and Levels

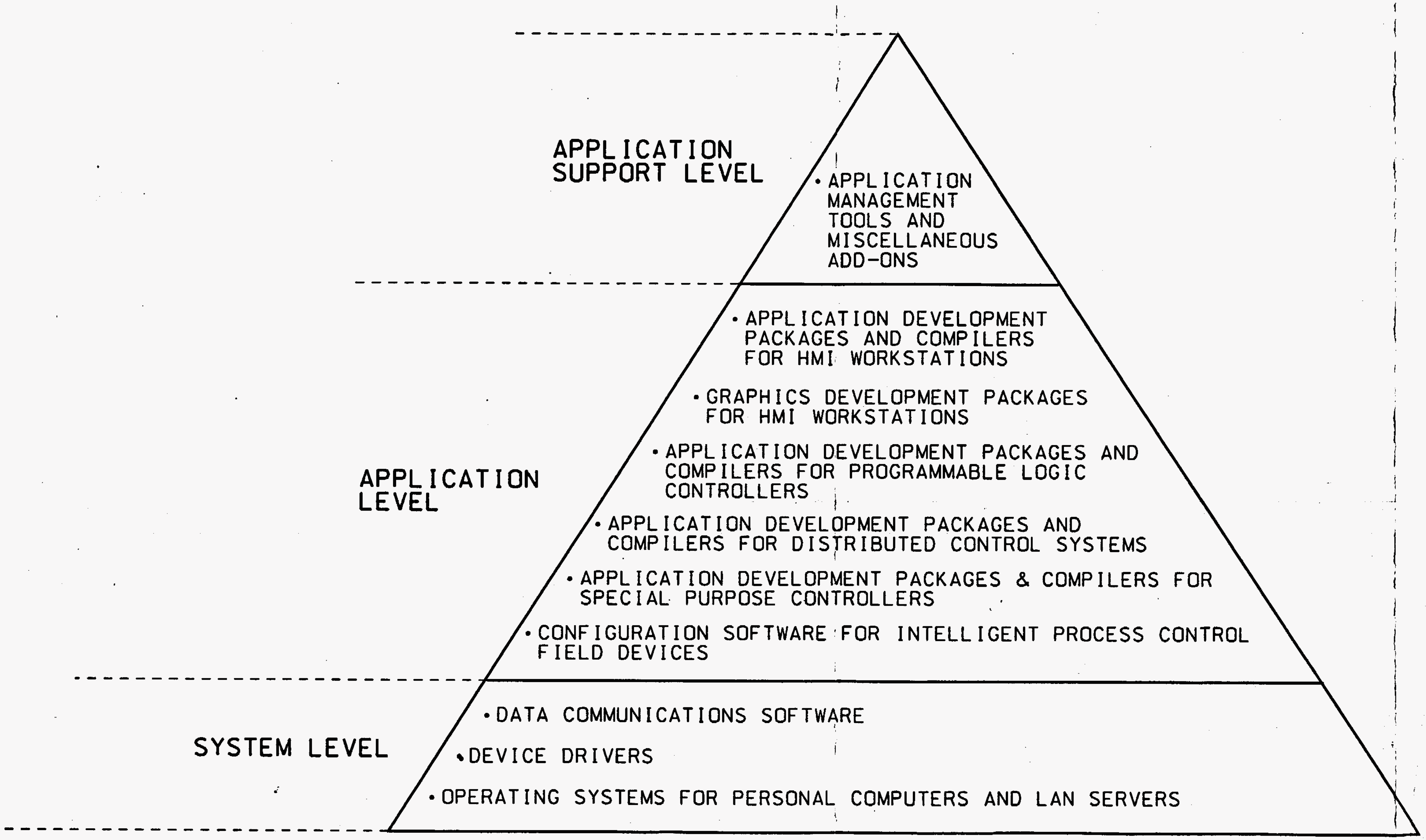
The Subsurface Repository Integrated Control System contains a wide variety of computer-based control components for all process and communications systems throughout the subsurface facility. As a direct result of this, the system will require a range of both manufacturer-supplied and custom-developed software routines and programs, as well as various commercial off-the-shelf application development packages to perform all required monitoring, control, and communication functions. The categories or types of software programs and development packages roughly correspond to the types of hardware components they are used with and the operational functions they serve. These software types include:

- Graphics development packages for HMI workstations
- Application development packages and compilers for HMI workstations
- Application development packages and compilers for DCSs
- Application development packages and compilers for PLCs

- Application development packages and compilers for special purpose controllers
- Configuration software for programmable process control field devices
- Configuration and network management software for data communications equipment
- Operating systems for PCs and LAN servers
- Application management tools and miscellaneous add-ons for PCs and LAN servers
- Device drivers for PC and LAN-server peripherals and accessories, and special purpose controllers

Many computer application programs will exist for process control and communications throughout the Subsurface Repository Integrated Control System. These software applications or program "blocks" are generally represented by the individual items shown on the monitoring/control level of control system functional block diagrams (Figures 1 through 18).

The various types of software listed above may be functionally organized into a triple-level pyramidal hierarchy as shown in Figure 28. The pyramid structure groups the software types into one of three different levels for the purpose of organizing each type according to its relative functional importance among the other types. These levels are the system level, the application level, and the application-support level. Each level in the pyramid is considered to be the platform or foundation for each of the levels resting on top of it. The system level or base of the pyramid is made up of the software types that allow all process computers to perform their elementary system functions, and to communicate with other devices as well as with each other. This software also, in a sense, integrates all monitoring and control programs for the Subsurface Repository Integrated Control System. It is where all process data throughout the subsurface are collected, managed, and distributed in the most fundamental ways. The application level represents the software required for the actual monitoring and control of all the different subsurface process systems. The application support level consists of whatever application development tools, diagnostic utilities, performance optimizers, database management and analysis aids, etc., that might be employed to support or enhance the applications residing at the level below.


APPLICATION SUPPORT LEVEL
• APPLICATION MANAGEMENT TOOLS AND MISCELLANEOUS ADD-ONS
APPLICATION LEVEL
• APPLICATION DEVELOPMENT PACKAGES AND COMPILERS FOR HMI WORKSTATIONS
• GRAPHICS DEVELOPMENT PACKAGES FOR HMI WORKSTATIONS
• APPLICATION DEVELOPMENT PACKAGES AND COMPILERS FOR PROGRAMMABLE LOGIC CONTROLLERS
• APPLICATION DEVELOPMENT PACKAGES AND COMPILERS FOR DISTRIBUTED CONTROL SYSTEMS
• APPLICATION DEVELOPMENT PACKAGES & COMPILERS FOR SPECIAL PURPOSE CONTROLLERS
• CONFIGURATION SOFTWARE FOR INTELLIGENT PROCESS CONTROL FIELD DEVICES
SYSTEM LEVEL
• DATA COMMUNICATIONS SOFTWARE
• DEVICE DRIVERS
• OPERATING SYSTEMS FOR PERSONAL COMPUTERS AND LAN SERVERS

t:*repss*csys*fig*sscs0123.fig

FIGURE 28
SOFTWARE TYPES AND LEVELS

FILE NAME: WO3969/CSYS/FIG/SSCS0123.FIG PD: 09/27/99

### 6.8.3 Regulatory and Industry Standards

Inasmuch as the software-based monitoring and control functions performed by the Subsurface Repository Integrated Control System will take place in a nuclear environment, it would be sound practice to examine the standards and regulations governing the use of software in control systems of commercial nuclear power generating stations. Such an examination and study would assist in determining the specific software planning, development, and design requirements for the Subsurface Repository Integrated Control System. Therefore, is recommended that a number of the IEEE standards pertaining to software in the nuclear power industry be consulted in order to establish these requirements for the Subsurface Repository Integrated Control System. These standards include IEEE Standard 730 (DIRS 41), IEEE Standard 730.1 (DIRS 42), IEEE Standard 828 (DIRS 43), ANSI/IEEE Standard 829 (DIRS 44), IEEE Standard 830 (DIRS 45), IEEE Standard 1008 (DIRS 46), IEEE Standard 1012 (DIRS 47), IEEE Standard 1016 (DIRS 48), IEEE Standard 1028 (DIRS 50), IEEE Standard 1042 (DIRS 51), IEEE Standard 1059 (DIRS 52), IEEE Standard 1063 (DIRS 53), and IEEE Standard 1074 (DIRS 54) (Section 4.3.2). Many of these standards have been endorsed by a number of U.S. Nuclear Regulatory Commission Regulatory Guides and NUREG reports. The Regulatory Guides include 1.168 (DIRS 65), 1.169 (DIRS 66), 1.170 (DIRS 67), 1.171 (DIRS 68), 1.172 (DIRS 69), and 1.173 (DIRS 70) (Section 4.3.3). The NUREG reports include NUREG/CR-6101 (DIRS 56), NUREG/CR-6263 (DIRS 57), NUREG/CR-6278 (DIRS 58), NUREG/CR-6294 (DIRS 59), NUREG/CR-6421 (DIRS 60), NUREG/CR-6463 Rev. 1 (DIRS 61), and NUREG/CR-6465 (DIRS 62) (Section 4.3.3).

Upon finalization of the compliance program guidance packages for the Yucca Mountain Project, all or some of these regulations and standards may define project design criteria and requirements for the Subsurface Repository Integrated Control System. Although these regulatory documents apply to the commercial nuclear power industry, it is likely that some portions of their content will be applicable to the Subsurface Repository Integrated Control System. Therefore, further review and study of the Regulatory Guides and NUREG reports previously mentioned is recommended.

## 7. CONCLUSIONS

This analysis identifies the preliminary subsurface instrumentation, control functions, and interfaces as described in the SDDs. The data, voice, and video links between site-based systems and the Subsurface Integrated Control System are also identified. The Subsurface Repository Integrated Control System functional block diagrams (Figures 1 through 18) show all the applicable SDDs in the top three layers: Site, Facility, and System. The various process systems interface with one another as described in the SDDs. These diagrams will serve as the principal development guide for the Subsurface Repository Integrated Control System design. The functional architecture is discussed in Section 6.2.

A number of SDDs used as input criteria in Section 4.2, are currently affected by TBVs. The impact of these TBVs on this analysis is that items on the primary function level of some of the functional block diagrams are unverified at the present time. The functional block diagrams affected depends upon which SDDs are affected by TBVs. All affected SDDs and their corresponding TBV numbers are given in Section 4.2.

The physical architecture of the Subsurface Repository Integrated Control System is based in part on the functions identified in the functional block diagrams. The physical architecture diagrams represent an initial effort to integrate all subsurface control systems and devices, and to establish the different levels of control that might be used in the subsurface repository. Also, the physical architecture diagrams provide an initial estimate of the complexity of the subsurface process control, voice communication, and video monitoring systems. These diagrams can also assist design engineers in planning their course of work more efficiently, as the Subsurface Repository Integrated Control System needs to be in place at the end of each cluster development cycle to complete the development of a cluster of emplacement drifts. The design presented in this analysis must be considered preliminary and will most likely undergo changes and refinements. The physical architecture is discussed in Section 6.3.

The Subsurface Repository Integrated Control System data communications design reflects the overall data communications portion of the physical architecture. Data communications are considered a key component of the Subsurface Repository Integrated Control System. This network serves as the physical link between all of the systems and devices throughout the subsurface facility. Data communications are discussed in Section 6.4.

The control room equipment arrangement and layout for the Subsurface Repository Integrated Control System is a modular concept designed according to system functionality. It comprises a number of supervisory consoles or expandable groups of operator monitoring and interface devices that are functionally related. Control room design for subsurface operations is discussed in Section 6.5.

The safety-critical functions of the Subsurface Repository Integrated Control System shall conform to a number of design aims related to safety. These strategic features include reliability, availability, fail-safe operation, system and data integrity, system recovery, maintainability, and dependability. Furthermore, since the safety-critical functions of the Subsurface Repository Integrated Control System are computer-based and will take place in a nuclear environment, the design requirements for the system shall comply with the standards and regulations governing the use of digital computers in commercial nuclear power plants. Safety strategies and requirements are discussed in Section 6.6.

The Subsurface Repository Integrated Control System must possess the capability to ensure an organized and planned response to what have been identified as off-normal events surrounding subsurface repository operations. Means of effecting responses to off-normal events shall include, as a minimum, alarm and notification systems, emergency shutdowns, emergency response plans, manual overrides, and backup power supplies. Off-normal events and responses are discussed in Section 6.7.

Due to the anticipated size and complexity of the configuration and computer programming tasks faced by the developers of the Subsurface Repository Integrated Control System, a software planning and development program shall be produced and implemented. Furthermore, inasmuch as the system software-based monitoring/control functions will take place in a nuclear environment, the system shall comply with the standards and regulations governing the use of control system software in commercial nuclear power plants. Software development strategies are discussed in Section 6.8.

Evolving technologies should be considered a key factor in the Subsurface Repository Integrated Control System design, as the positive changes in technology could provide greater reliability and reduce system complexity.

Some SDDs used in this analysis have a global to-be-verified (TBV) designation. However, these sources are offered as design inputs to this analysis since only primary system functions are cited and, thus, should not impact the conclusions of this analysis. The design configurations presented in this analysis will need to be re-evaluated after all the relevant SDDs receive Level 3 Change Control Board approval.

Specific conclusions that can be drawn from this analysis are as follows:

- The data communications backbone for the Subsurface Repository Integrated Control System shall have at least one redundancy level for all non-safety-critical functions.
- The Subsurface Repository Integrated Control System shall conform to an open system architecture.
- The control functions of the Subsurface Repository Integrated Control System should be distributed (decentralized) in order to avoid single-point failures and provide easy maintenance and upgrades.
- The data communications for the Subsurface Repository Integrated Control System shall be deterministic.
- The data communications system backbone for the Subsurface Repository Integrated Control System shall have more than one redundancy level for safety-critical functions.
- The Subsurface Repository Integrated Control System shall be diverse in the design of its subsystems and components, and physical separation of system components shall be practiced in order to reduce common-cause failures.
- Future work shall be considered to develop or site-wide (surface and subsurface) network integration architectures. It is recommended that the Respository Surface, Repository Subsurface, and Repository Systems Operation groups collaborate in this effort. These integration issues are identified and discussed in the *Monitored Geologic Repository Instrumentation and Control System Strategy* document (DIRS 35).
- The design development of the Subsurface Repository Integrated Control System shall consider the application of human factors to system operations, and appropriate measures shall be taken to reduce the potential for human operational errors.
- The design development of the various process control computers and data communications networks of the Subsurface Repository Integrated Control System shall allow for the expansion of additional process control hardware and software with minimum impact to existing systems.

- The design development of the Subsurface Repository Integrated Control System shall include a formal risk analysis.

- A formal specification of the safety requirements of the Subsurface Repository Integrated Control System shall be developed as part of the future design.

- A formal single-failure analysis shall be performed during the design of the Subsurface Repository Integrated Control System. The single-failure analysis shall be performed in conjunction with a comprehensive facility analysis of the MGR.

- A formal reliability analysis of the safety features of the Subsurface Repository Integrated Control System shall be performed as part of the future design.

- A computer software and hardware quality assurance plan shall be developed for the Subsurface Repository Integrated Control System as part of the future design.

- A software planning and development program shall be produced and implemented for the Subsurface Repository Integrated Control System as part of the future design.

- A computer software configuration management plan shall be developed for the Subsurface Repository Integrated Control System as part of the future design.

- A computer software verification and validation plan shall be developed for the Subsurface Repository Integrated Control System as part of the future design.

- The Subsurface Repository Integrated Control System design shall incorporate proven state-of-the-art technologies in controls and communications. Furthermore, the system shall be designed in a manner that can accommodate advancements and proven innovations in controls and communication technologies.

## ATTACHMENTS

| **Attachment** | **Title** |
|---|---|
| I | *Document Input Reference Sheets (DIRS)* |

# ATTACHMENT I

# DOCUMENT INPUT REFERENCE SHEETS (DIRS)

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| 2. Technical Product Input Source Title and Identifier(s) with Version | | 3. Section | | | | | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>1 | CRWMS M&O 1998. *Subsurface Ventilation System Description Document*. BCA000000-01717-1705-00016 REV 00, ICN 1. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19980511.0220, MOL.19981117.0420. | Vol. I, 1.1.1 | N/A | 6.2.2.8 | Air flow generation and control | N/A | | | |
| 1 | | Vol. I, 1.1.2 | N/A | 6.2.2.8 | Air quality maintenance | N/A | | | |
| 1 | | Vol. I, 1.1.3 | N/A | 6.2.2.8 | Air cleanup and filtration | N/A | | | |
| 1 | | Vol. I, 1.1.4 | N/A | 6.2.2.8 | Air temperature control | N/A | | | |
| 1 | | Vol. I, 1.1.5 | N/A | 6.2.2.8 | Containment of radioactive contaminants | N/A | | | |
| 1 | | Vol. I, 1.1.6 | N/A | 6.2.2.8 | Human access control | N/A | | | |
| 1 | | Vol. I, 1.1.7 | N/A | 6.2.2.8 | System and equipment monitoring | N/A | | | |
| 1 | | Vol. I, 1.1.10 | N/A | 6.2.2.8 | Data transfer to facility control systems | N/A | | | |
| 1 | | Vol. I, 1.1.11 | N/A | 6.2.2.8 | Combustion products containment | N/A | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | | | | | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2. Technical Product Input Source Title and Identifier(s) with Version | 3. Section | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>2 | CRWMS M&O 1998. *Waste Emplacement System Description Document*. BCA000000-01717-1705-00017 REV 00. Las Vegas, Nevada: CRWMS M&O ACC: MOL.19980519.0234. | Vol. 1, 1.1.1 | N/A | 6.2.2.2 | Waste package receipt | N/A | | | |
| 2 | | Vol. 1, 1.1.2 | N/A | 6.2.2.2 | Waste package transport | N/A | | | |
| 2 | | Vol. 1, 1.1.3 | N/A | 6.2.2.2 | Waste package emplacement | N/A | | | |
| 2 | | Vol. 1, 1.1.4 | N/A | 6.2.2.2 | Waste package removal and relocation | N/A | | | |
| 2 | | Vol. I, 1.1.5 | N/A | 6.2.2.2 | Remote control capabilities | N/A | | | |
| 2 | | Vol. 1, 1.1.6 | N/A | 6.2.2.2 | Remote visual surveillance | N/A | | | |
| 2 | | Vol. 1, 1.1.7 | N/A | 6.2.2.2 | System interfaces | N/A | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2. Technical Product Input Source Title and Identifier(s) with Version | 3. Section | | | | | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>3 | OCRWM 1999. Input Transmittal, Input Tracking No. EBS-RSO-99298.T for the *Monitored Geologic Repository (MGR) Operations Monitoring and Control System Description Document (SDD)*. BCA000000-01717-1705-00001 REV 00A. Las Vegas, Nevada: OCRWM ACC: MOL.19990928.0101. | Vol. I, 1.1.1 | TBV-3759 | 6.5 | Subsurface operations monitoring and control room | 2 | X | | |
| 3 | | Vol. I, 1.1.2 | TBV-3759 | 6.2.2.8 | Subsurface ventilation system supervisory control | 2 | X | | |
| 3 | | Vol. I, 1.1.3 | TBV-3759 | 6.2.2.12 and 6.2.2.13 | Subsurface utilities supervisory control | 2 | X | | |
| 3 | | Vol. I, 1.1.6 | TBV-3759 | 6.7.3 | Shutdown of subsurface systems | 2 | X | | |
| 3 | | Vol. I, 1.1.7 | TBV-3759 | 6.2.2.2 and 6.2.2.3 | Waste emplacement safety systems status monitoring | 2 | X | | |
| 3 | | Vol. I, 1.1.8 | TBV-3759 | 6.7.1 and 6.2.2.1 | Subsurface safety systems monitoring and control | 2 | X | | |
| 3 | | Vol. I, 1.1.9 | TBV-3759 | 6.7.3 and 6.2.2.1 | Subsurface facility operational startup | 2 | X | | |
| 3 | | Vol. I, 1.1.10 | TBV-3759 | 6.7.3 and 6.2.2.1 | Alarms for off-normal conditions | 2 | X | | |
| 3 | | Vol. I, 1.1.11 | TBV-3759 | 6.2.2.1 | Subsurface equipment performance monitoring | 2 | X | | |
| 3 | | Vol. I, 1.1.2 | TBV-3759 | 6.2.2.1 | System interfaces | 2 | X | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| 1. Document Identifier No./Rev.: | Change: | Title: |
|---|---|---|
| ANL-MGR-CS-000001/REV 00 | N/A | Subsurface Repository Integrated Control System Design |

| Input Document | | | | | | | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| 2. Technical Product Input Source Title and Identifier(s) with Version | | 3. Section | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | Unqual. | From Uncontrolled Source | Un-confirmed |
| 3 | OCRWM 1999. Input Transmittal, Input Tracking No. EBS-RSO-99298.T for the *Monitored Geologic Repository (MGR) Operations Monitoring and Control System Description Document (SDD).* BCA000000-01717-1705-00001 REV 00A. Las Vegas, Nevada: OCRWM ACC: MOL.19990928.0101. | Vol. I, 1.1.13 | TBV-3759 | 6.2.2.11 | Subsurface communications | 2 | X | | |
| 3 | | Vol. I, 1.1.14 | TBV-3759 | 6.2.2.5 | Radioactive effluents monitoring and tracking | 2 | X | | |
| 3 | | Vol. I, 1.1.16 | TBV-3759 | 6.2.2.9 | Subsurface environmental data monitoring | 2 | X | | |
| 3 | | Vol. I, 1.1.17 | TBV-3759 | 6.2.2.2 and 6.2.2.4 | Remote control of waste emplacement and performance confirmation operations | 2 | X | | |
| 3 | | Vol. I, 1.2.1.9 | TBV-3759 | 6.2.2.9 | Subsurface radiation alarms | 2 | X | | |
| 3 | | Vol. I, 1.2.1.11 | TBV-3759 | 6.2.2.8 | Subsurface differential pressure monitoring | 2 | X | | |
| 3 | | Vol. I, 1.2.1.15 | TBV-3759 | 6.2.2.2 | Subsurface isolation door monitoring | 2 | X | | |
| 3 | | Vol. I, 1.2.1.22 | TBV-3759 | 6.2.2.1 | Subsurface remote operations monitoring | 2 | X | | |
| 3 | | Vol. I, 1.2.1.23 | TBV-3759 | 6.2.2.1 | Subsurface operations data storage | 2 | X | | |
| 3 | | Vol. I, 1.2.1.27 | TBV-3759 | 6.2.2.1 and 6.3.1.10 | Hardware and software expansion capabilities | 2 | X | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| 2. Technical Product Input Source Title and Identifier(s) with Version | | 3. Section | | | | | Unqual. | From Uncontrolled Source | Un-confirmed |
| 3 | OCRWM 1999. Input Transmittal, Input Tracking No. EBS-RSO-99298.T for the *Monitored Geologic Repository (MGR) Operations Monitoring and Control System Description Document (SDD)*. BCA000000-01717-1705-00001 REV 00A. Las Vegas, Nevada: OCRWM ACC: MOL.19990928.0101. | Vol. I, 1.2.2.1.9 | TBV-3759 | 6.3.1.4 | Common-cause failures | 2 | X | | |
| 3 | | Vol. I, 1.2.2.1.17 | TBV-3759 | 6.2.2.9 | Subsurface radiation monitoring | 2 | X | | |
| 3 | | Vol. I, 1.2.2.1.19 | TBV-3759 | 6.2.2.9 | Subsurface radiation alarm system | 2 | X | | |
| 3 | | Vol. I, 1.2.2.1.20 | TBV-3759 | 6.3.1.4, 6.6.2.1 | Control system redundancy and single failures | 2 | X | | |
| 3 | | Vol. I, 1.2.2.1.21 | TBV-3759 | 6.2.2.8 | Subsurface differential pressure monitoring | 2 | X | | |
| 3 | | Vol. I, Summary | TBV-3759 | 6.2.2.1 | System interfaces | 2 | X | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| 2. Technical Product Input Source Title and Identifier(s) with Version | | 3. Section | | | | | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>4 | CRWMS M&O 1998. *Ground Control System Description Document.* BCA000000-01717-1705-00011. Rev. 00. Las Vegas, Nevada: CRWMS M&O ACC: MOL.19980825.0286. | Vol. I, 1.1.3 | N/A | 6.2.2.14 | Ground control components and rock monitoring | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | | | | | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2. Technical Product Input Source Title and Identifier(s) with Version | 3. Section | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>5 | CRWMS M&O 1998. *Performance Confirmation Emplacement Drift Monitoring System Description Document.* BCA000000-01717-1705-00020 Rev. 00. Las Vegas, Nevada: CRWMS M&O ACC: MOL.19981117.0426. | Vol. I, 1.1.1 | N/A | 6.2.2.4 | Emplacement drift and waste package monitoring | N/A | | | |
| 5 | | Vol. I, 1.1.2 | N/A | 6.2.2.4 | Emplacement drift environmental conditions monitoring | N/A | | | |
| 5 | | Vol. I, 1.1.3 | N/A | 6.2.2.4 | Waste package conditions monitoring | N/A | | | |
| 5 | | Vol. I, 1.1.4 | N/A | 6.2.2.4 | Emplacement drift and waste package data transfer | N/A | | | |
| 5 | | Vol. I, 1.1.5 | N/A | 6.2.2.4 | Emplacement drift test coupons | N/A | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| 2. Technical Product Input Source Title and Identifier(s) with Version | | 3. Section | | | | | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>6 | CRWMS M&O 1998. *Waste Retrieval System Description Document.* BCA000000-01717-1705-00018 Rev. 00. Las Vegas, Nevada: CRWMS M&O ACC: MOL.19980903.0869. | Vol. I, 1.1.1 | N/A | 6.2.2.6 | Normal waste package retrieval | N/A | | | |
| 6 | | Vol. I, 1.1.2 | N/A | 6.2.2.6 | Normal/abnormal select waste package retrieval | N/A | | | |
| 6 | | Vol. I, 1.1.3 | N/A | 6.2.2.6 | Abnormal waste package retrieval during emplacement | N/A | | | |
| 6 | | Vol. I, 1.1.4 | N/A | 6.2.2.6 | Debris and equipment removal | N/A | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| 2. Technical Product Input Source Title and Identifier(s) with Version | | 3. Section | | | | | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>7 | CRWMS M&O 1998. *Backfill Emplacement System Description Document.* BCA000000-01717-1705-00010 Rev. 00. Las Vegas, Nevada: CRWMS M&O ACC: MOL.19981111.0001. | Vol. I, 1.1.2 | N/A | 6.2.2.7 | Backfill material transport | N/A | | | |
| 7 | | Vol. I, 1.1.3 | N/A | 6.2.2.7 | Backfill material emplacement | N/A | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | | | | | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| 2. Technical Product Input Source Title and Identifier(s) with Version | | 3. Section | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>8 | OCRWM 1999. Input Transmittal, Input Tracking No. ESB-SEI-99255.T for the *Performance Confirmation Data Acquisition/ Monitoring System Description Document.* BCB000000-01717-1705-00034 Rev. 00. Las Vegas, Nevada: OCRWM ACC: MOL.19990826.0071. | Vol. I, 1.1.4 | TBV-407 | 6.2.2.5 | Excavation and borehole parameter monitoring | 2 | X | | |
| 8 | | Vol. I, 1.1.5 | TBV-407 | 6.2.2.5 | Waste package parameter monitoring | 2 | X | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2. Technical Product Input Source Title and Identifier(s) with Version | 3. Section | | | | | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>9 | CRWMS M&O 1999. *Subsurface Fire Protection System Description Document.* BCA00000-01717-1705-00006 Rev 00. Las Vegas, Nevada: CRWMS M&O ACC: MOL.19990720.0206. | Vol. I, 1.1.1 | N/A | 6.2.2.10 | Personnel and equipment protection from subsurface fires | 2 | X | | |
| 9 | | Vol. I, 1.1.2 | N/A | 6.2.2.10 | Control of subsurface fires | 2 | X | | |
| 9 | | Vol. I, 1.1.3 | N/A | 6.2.2.10 | Detection and annunciation of subsurface fires | 2 | X | | |
| 9 | | Vol. I, 1.1.4 | N/A | 6.2.2.10 | Subsurface fire suppression | 2 | X | | |
| 9 | | Vol. I, 1.1.5 | N/A | 6.2.2.10 | Detection, control, and mitigation of subsurface explosion hazards | 2 | X | | |
| 9 | | Vol. I, 1.1.6 | N/A | 6.2.2.10 | Notification of subsurface fires | 2 | X | | |

# OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT

## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2. Technical Product Input Source Title and Identifier(s) with Version | 3. Section | | | | | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>10 | CRWMS M&O 1999. *Subsurface Electrical Distribution System Description Document*. BCA000000-01717-1705-00005 Rev 00. Las Vegas, Nevada: CRWMS M&O ACC: MOL.19990609.0155. | Vol. I, 1.1.1 | N/A | 6.2.2.12 | Subsurface electrical power distribution | 2 | X | | |
| 10 | | Vol. I, 1.1.3 | N/A | 6.2.2.12 | Subsurface electrical power monitoring | 2 | X | | |
| 10 | | Vol. I, 1.1.5 | N/A | 6.2.2.12 | Subsurface normal and standby power distribution | 2 | X | | |
| 10 | | Vol. I, 1.1.6 | N/A | 6.2.2.12 | Subsurface electrical power distribution | 2 | X | | |
| 10 | | Vol. I, 1.1.7 | N/A | 6.2.2.12 | Provisions for subsurface lighting, . grounding, and lightning protection | 2 | X | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2. Technical Product Input Source Title and Identifier(s) with Version | 3. Section | | | | | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>11 | CRWMS M&O 1999. *Subsurface Excavation System Description Document.* BCA00000-01717-1705-00003 Rev 00. Las Vegas, Nevada: CRWMS M&O ACC: MOL.19990429.0227. | Vol. I, 1.1.1 | N/A | 6.2.2.14 | Subsurface opening excavation | 2 | X | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| 2. Technical Product Input Source Title and Identifier(s) with Version | | 3. Section | | | | | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>12 | Initial Issue | N/A | TBV-406 | 5 | Primary functions of the Subsurface Emplacement Transportation System | 3 | X | X | X |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | | | | | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2. Technical Product Input Source Title and Identifier(s) with Version | 3. Section | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>13 | Initial Issue | N/A | TBV-409 | 5 | Primary functions of the Subsurface Compressed Air System. | 3 | X | X | X |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2. Technical Product Input Source Title and Identifier(s) with Version | 3. Section | | | | | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>14 | Initial Issue | N/A | TBV-411 | 5 | Primary functions of the Subsurface Water Collection/Removal System | 3 | X | X | X |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| 2. Technical Product Input Source Title and Identifier(s) with Version | | 3. Section | | | | | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>15 | Initial Issue | N/A | TBV-415 | 5 | Primary functions of the Subsurface Water Distribution System | 3 | X | X | X |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | | | | | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| 2. Technical Product Input Source Title and Identifier(s) with Version | | 3. Section | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>16 | Initial Issue | N/A | TBV-417 | 5 | Primary functions of the Muck Handling System | 3 | X | X | X |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | | | | | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| 2. Technical Product Input Source Title and Identifier(s) with Version | | 3. Section | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>17 | Initial Issue | N/A | TBV-1213 | 5 | Primary functions of the Subsurface Development Transportation System | 3 | X | X | X |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | | Change:<br>N/A | | Title:<br>Subsurface Repository Integrated Control System Design | | | | | |
| Input Document | | | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | 8. TBV Due To | | |
| | 2. Technical Product Input Source Title and Identifier(s) with Version | 3. Section | | | | | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>18 | Albus, J., Quintero, R., Huang, H., and Roche, M. 1989. NIST Technical Note 1261 Volume 1 *Mining Automation Real-Time Control System Architecture Standard Reference Model (MASREM).* NISTTN 1261, Volume 1. Gaithersburg, MD: National Institute of Standards and Technology. TIC: 239469. | Total doc. | N/A | 6.2 | NIST functional architecture technique | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | | | | | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2. Technical Product Input Source Title and Identifier(s) with Version | 3. Section | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>19 | CRWMS M&O 1997. *Emplacement System Control and Communication Analysis.* BCA000000-01717-0200-00016 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19980113.0786. | Total doc. | N/A | 1.0,<br>6.2.2.2,<br>6.2.2.11 | Emplacement system equipment controls | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

1. Document Identifier No./Rev.: ANL-MGR-CS-000001/REV 00

Change: N/A

Title: Subsurface Repository Integrated Control System Design

| Input Document | | | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2. Technical Product Input Source Title and Identifier(s) with Version | 3. Section | | | | | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>20 | CRWMS M&O 1998. *Site Communications and Control Systems Technical Report*. BCBC00000-01717-5705-00002 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19980702.0410. | Total doc. | N/A | 6.3.1.8 | Surface administrative functions | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | | | | | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2. Technical Product Input Source Title and Identifier(s) with Version | 3. Section | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>21 | CRWMS M&O 1997. *Performance Confirmation Data Acquisition System.* BCAI00000-01717-0200-00002 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19980513.0133. | Total doc | N/A | 1.0,<br>6.2.2.5,<br>6.2.2.14 | Performance confirmation system monitored parameters and instrumentation | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| 2. Technical Product Input Source Title and Identifier(s) with Version | | 3. Section | | | | | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>22 | CRWMS M&O 1997. *Transport and Emplacement Equipment Descriptions*. BCAF00000-01717-5705-00002 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19980106.0571. | Total doc. | N/A | 1.0, 6.2.2.2 | Waste emplacement system equipment | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Input Document | | | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | 8. TBV Due To | | |
| | 2. Technical Product Input Source Title and Identifier(s) with Version | 3. Section | | | | | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>23 | CRWMS M&O 1997. *Evaluation of Waste Package Transport and Emplacement Equipment.* BCAF00000-01717-0200-00002 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19971201.0869. | Total doc. | N/A | 1.0,<br>6.2.2.2 | Waste emplacement system equipment | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT

## DOCUMENT INPUT REFERENCE SHEET

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | | | Change:<br>N/A | | Title:<br>Subsurface Repository Integrated Control System Design | | | | |
| Input Document | | | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | 8. TBV Due To | | |
| 2. Technical Product Input Source Title and Identifier(s) with Version | | 3. Section | | | | | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>24 | CRWMS M&O 1997. *Subsurface Waste Package Handling – Remote Control and Data Communications Analysis.* BCA000000-01717-0200-00004 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19970714.0655. | Total doc. | N/A | 1.0, 6.2.2.2, 6.2.2.11, 6.4.3 | Emplacement system equipment controls and data communications | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | | | | | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| 2. Technical Product Input Source Title and Identifier(s) with Version | | 3. Section | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>25 | CRWMS M&O 1997. *Repository Rail Electrification Analysis.* BCAC00000-01717-0200-00002 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19980122.0462. | Total doc. | N/A | 6.2.2.3 | Rail transportation system power | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Input Document | | | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | 8. TBV Due To | | |
| 2. Technical Product Input Source Title and Identifier(s) with Version | | 3. Section | | | | | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>26 | CRWMS M&O 1998. *Site Electrical System Technical Report*. BCBC00000-01717-5705-00003 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19980702.0372. | Total doc. | N/A | 6.2.2.12 | Electrical power distribution equipment | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | | | | | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2. Technical Product Input Source Title and Identifier(s) with Version | 3. Section | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>27 | CRWMS M&O 1999. *Monitored Geologic Repository Architecture.* B00000000-01717-5700-00011 REV 03 ICN 01. Las Vegas, Nevada: CRWMS M&O ACC: MOL.19991101.0211. | Total doc. | N/A | 6.2.2.1 | MGR architecture | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | | Change:<br>N/A | | Title:<br>Subsurface Repository Integrated Control System Design | | | | | |
| Input Document | | | | | | | 8. TBV Due To | | |
| | 2. Technical Product Input Source Title and Identifier(s) with Version | 3. Section | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>28 | CRWMS M&O 1999. Activity Evaluation, *SS Transport & Emplacement – 99 Work Package 12012383M1.* Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19990413.0017. | Total doc. | N/A | 2.0 | Conduct of activities | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| 2. Technical Product Input Source Title and Identifier(s) with Version | | 3. Section | | | | | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>29 | OCRWM 1998. *Quality Assurance Requirements and Description.* DOE/RW-0333P, Rev 8. Washington D.C.: U.S. Department of Energy, Office of Civilian Radioactive Waste Management. ACC: MOL.19980601.0022. | Total doc. | N/A | 2.0 | Quality assurance requirements | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2. Technical Product Input Source Title and Identifier(s) with Version | 3. Section | | | | | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>30 | CRWMS M&O 1997. *Subsurface Construction and Development Analysis.* BCA000000-01717-0200-00014 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19971210.0560. | Total doc. | N/A | 6.2.2.14 | Subsurface development transportation system equipment | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | | | | | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2. Technical Product Input Source Title and Identifier(s) with Version | 3. Section | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>31 | OCRWM 1999. *Classification of the MGR Operations Monitoring and Control System*. ANL-OMC-SE-000001 REV 00. Las Vegas, Nevada: OCRWM. ACC: MOL.19990927.0474. | Total doc. | N/A | 2.0 | QA classification | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | | | | | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2. Technical Product Input Source Title and Identifier(s) with Version | 3. Section | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>32 | U. S. Department of Energy December 1998. *Viability Assessment of a Repository at Yucca Mountain - Preliminary Design Concept for the Repository and Waste Package, Volume 2*. DOE/RW-0508. ACC: MOL.19981007.0029. | 5.3.1 | N/A | 6.2.2.7 | Backfill emplacement system operations | N/A | | | |
| 32 | | 4.2.4 | N/A | 6.2.2.8 | Subsurface ventilation system operations | N/A | | | |
| | | | | | | | | | |

**OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT**

**DOCUMENT INPUT REFERENCE SHEET**

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | | | | | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2. Technical Product Input Source Title and Identifier(s) with Version | 3. Section | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>33 | CRWMS M&O 1998. *Retrieval Equipment and Strategy.* BCAF00000-01717-0200-00008 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19990414.0212. | Total doc. | N/A | 6.2.2.6 | Waste retrieval equipment | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | | | | | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2. Technical Product Input Source Title and Identifier(s) with Version | 3. Section | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>34 | CRWMS M&O 1998. *Repository Subsurface Control Integration Plan.* BCAC00000-01717-4600-00001 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19990223.0154. | Total doc. | N/A | 6.8.1 | Software planning and development program | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2. Technical Product Input Source Title and Identifier(s) with Version | 3. Section | | | | | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>35 | CRWMS M&O 1999. Monitored Geologic *Repository Instrumentation and Control System Strategy*. BA0000000-01717-5700-00023 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19990505.0448. | Total doc. | N/A | 6.3.1.4 | Control system redundancy | N/A | | | |
| 35 | | Total doc. | N/A | 6.3.1.9,<br>6.6 | Control system safety | N/A | | | |
| 35 | | Total doc. | N/A | 6.3.1.14 | Control system reliability | N/A | | | |
| 35 | | Total doc. | N/A | 6.7.1 | Off-normal events | N/A | | | |
| 35 | | Total doc. | N/A | 7 | Control system integration | N/A | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2. Technical Product Input Source Title and Identifier(s) with Version | 3. Section | | | | | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>36 | ASME NQA-1-1997. *Quality Assurance Program Requirements for Nuclear Facility Applications*. New York, New York: The American Society of Mechanical Engineers. Readily available. | Total doc. | N/A | 6.6.2.3 | Quality assurance requirements for nuclear facilities | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| 2. Technical Product Input Source Title and Identifier(s) with Version | | 3. Section | | | | | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>37 | IEEE Std 7-4.3.2-1993. *IEEE Standard for Digital Computers in Safety Systems of Nuclear Power Generating Stations.* New York, New York: The Institute of Electrical and Electronics Engineers, Inc. Readily available. | Total doc. | N/A | 6.6.2 | Digital computers in safety systems for nuclear power generating stations. | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | | | | | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2. Technical Product Input Source Title and Identifier(s) with Version | 3. Section | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>38 | IEEE Std 352-1987. *IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Protection Systems*. New York, New York: The Institute of Electrical and Electronics Engineers, Inc. Readily available. | Total doc. | N/A | 6.6.2.13 | Reliability analysis of nuclear power generating stations. | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | | | | | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2. Technical Product Input Source Title and Identifier(s) with Version | 3. Section | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a | | | | | | | | | |
| 39 | IEEE Std 577-1976. *IEEE Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Power Generating Stations*. New York, New York: The Institute of Electrical and Electronics Engineers, Inc. Readily available. | Total doc. | N/A | 6.6.2.13 | Reliability analysis in safety systems for nuclear power generating stations | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2. Technical Product Input Source Title and Identifier(s) with Version | 3. Section | | | | | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>40 | IEEE Std 603-1991. *IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations*. New York, New York: The Institute of Electrical and Electronics Engineers, Inc. Readily available. | Total doc. | N/A | 6.6.2 | Safety systems for nuclear power generating stations. | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | | | | | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2. Technical Product Input Source Title and Identifier(s) with Version | 3. Section | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>41 | IEEE Std 730-1998. *IEEE Standard for Software Quality Assurance Plans*. New York, New York: The Institute of Electrical and Electronics Engineers, Inc. Readily available. | Total doc. | N/A | 6.6.2.3, 6.8.3 | Software quality assurance plans. | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | | | | | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2. Technical Product Input Source Title and Identifier(s) with Version | 3. Section | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>42 | IEEE Std 730.1-1995. *IEEE Guide for Software Quality Assurance Planning.* New York, New York: The Institute of Electrical and Electronics Engineers, Inc. Readily available. | Total doc. | N/A | 6.6.2.3, 6.8.3 | Software quality assurance planning. | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2. Technical Product Input Source Title and Identifier(s) with Version | 3. Section | | | | | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>43 | IEEE Std 828-1990. *IEEE Standard for Software Configuration Management Plans.* New York, New York: The Institute of Electrical and Electronics Engineers, Inc. Readily available. | Total doc. | N/A | 6.6.2.3,<br>6.8.3 | Software configuration management plans. | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2. Technical Product Input Source Title and Identifier(s) with Version | 3. Section | | | | | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>44 | ANSI/IEEE Std 829-1983. *IEEE Standard for Software Test Documentation*. New York, New York: The Institute of Electrical and Electronics Engineers, Inc. Readily available. | Total doc. | N/A | 6.8.3 | Software test documentation. | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | | | | | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| 2. Technical Product Input Source Title and Identifier(s) with Version | | 3. Section | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>45 | IEEE Std 830-1993. *IEEE Recommended Practice for Software Requirements Specifications.* New York, New York: The Institute of Electrical and Electronics Engineers, Inc. Readily available. | Total doc. | N/A | 6.8.3 | Software requirements. | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

# OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT

## DOCUMENT INPUT REFERENCE SHEET

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | | | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design | | | | | |
| Input Document | | | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | 8. TBV Due To | | |
| 2. Technical Product Input Source Title and Identifier(s) with Version | | 3. Section | | | | | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>46 | IEEE Std 1008-1987. *IEEE Standard for Software Unit Testing*. New York, New York: The Institute of Electrical and Electronics Engineers, Inc. Readily available. | Total doc. | N/A | 6.8.3 | Software testing. | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| 2. Technical Product Input Source Title and Identifier(s) with Version | | 3. Section | | | | | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>47 | IEEE Std 1012-1986. *IEEE Standard for Software Validation and Verification Plans*. New York, New York: The Institute of Electrical and Electronics Engineers, Inc. Readily available. | Total doc. | N/A | 6.6.2.3, 6.8.3 | Software validation and verification plans. | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | | | | | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2. Technical Product Input Source Title and Identifier(s) with Version | 3. Section | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>48 | IEEE Std 1016-1987. *IEEE Recommended Practice for Software Design Descriptions.* New York, New York: The Institute of Electrical and Electronics Engineers, Inc. Readily available. | Total doc. | N/A | 6.8.3 | Software design descriptions. | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| 2. Technical Product Input Source Title and Identifier(s) with Version | | 3. Section | | | | | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>49 | IEEE Std 1023-1988. *IEEE Guide for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations.* New York, New York: The Institute of Electrical and Electronics Engineers, Inc. Readily available. | Total doc. | N/A | 6.6.2.12 | Human factors engineering of nuclear power generating stations. | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2. Technical Product Input Source Title and Identifier(s) with Version | 3. Section | | | | | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>50 | IEEE Std 1028-1988. *IEEE Standard for Software Reviews and Audits*. New York, New York: The Institute of Electrical and Electronics Engineers, Inc. Readily available. | Total doc. | N/A | 6.8.3 | Software reviews and audits. | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| 1. Document Identifier No./Rev.: | Change: | Title: |
|---|---|---|
| ANL-MGR-CS-000001/REV 00 | N/A | Subsurface Repository Integrated Control System Design |

| | Input Document | | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2. Technical Product Input Source Title and Identifier(s) with Version | 3. Section | | | | | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>51 | IEEE Std 1042-1987. *IEEE Guide to Software Configuration Management*. New York, New York: The Institute of Electrical and Electronics Engineers, Inc. Readily available. | Total doc. | N/A | 6.6.2.3, 6.8.3 | Software configuration management. | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| 2. Technical Product Input Source Title and Identifier(s) with Version | | 3. Section | | | | | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>52 | IEEE Std 1059-1993. *IEEE Guide for Software Verification and Validation Plans*. New York, New York: The Institute of Electrical and Electronics Engineers, Inc. Readily available. | Total doc. | N/A | 6.8.3 | Software verification and validation plans. | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| 2. Technical Product Input Source Title and Identifier(s) with Version | | 3. Section | | | | | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>53 | IEEE Std 1063-1987. *IEEE Standard for Software User Documentation*. New York, New York: The Institute of Electrical and Electronics Engineers, Inc. Readily available. | Total doc. | N/A | 6.8.3 | Software user documentation. | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2. Technical Product Input Source Title and Identifier(s) with Version | 3. Section | | | | | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>54 | IEEE Std 1074-1995. *IEEE Standard for Developing Software Life Cycle Processes.* New York, New York: The Institute of Electrical and Electronics Engineers, Inc. Readily available. | Total doc. | N/A | 6.8.3 | Software life-cycle processes. | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2. Technical Product Input Source Title and Identifier(s) with Version | 3. Section | | | | | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a | Not Used | | | | | | | | |
| 55 | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | | | | | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2. Technical Product Input Source Title and Identifier(s) with Version | 3. Section | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>56 | NUREG/CR-6101. 1993. *Software Reliability and Safety in Nuclear Reactor Protection Systems.* Livermore, California: Lawrence Livermore National Laboratory. Readily available. | Total doc. | N/A | 6.8.3 | Software reliability and safety in nuclear reactor protection systems. | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | | | | | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2. Technical Product Input Source Title and Identifier(s) with Version | 3. Section | 4. Input Status | 5. Section Used in | 6. Input Description | '7. TBV/TBD Priority | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>57 | NUREG/CR-6263. 1995. *High Integrity Software for Nuclear Power Plants.* McLean, Virginia: The MITRE Corporation. Readily available. | Total doc. | N/A | 6.8.3 | High-integrity software for nuclear power plants. | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | | Change:<br>N/A | | Title:<br>Subsurface Repository Integrated Control System Design | | | | | |
| Input Document | | | | | | | 8. TBV Due To | | |
| 2. Technical Product Input Source Title and Identifier(s) with Version | | 3. Section | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>58 | NUREG/CR-6278. 1994. *Survey of Industry Methods for Producing Highly Reliable Software.* Livermore, California: Lawrence Livermore National Laboratory. Readily available. | Total doc. | N/A | 6.8.3 | Industry methods for producing highly reliable software. | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | | | | | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2. Technical Product Input Source Title and Identifier(s) with Version | 3. Section | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>59 | NUREG/CR-6294. 1994. *Design Factors for Safety-Critical Software.* Livermore, California: Lawrence Livermore National Laboratory. Readily available. | Total doc. | N/A | 6.8.3 | Design factors for safety-critical software. | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2. Technical Product Input Source Title and Identifier(s) with Version | 3. Section | | | | | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>60 | NUREG/CR-6421. 1996. *A Proposed Acceptance Process for Commercial Off-the-Shelf (COTS) Software in Reactor Applications.* Livermore, California: Lawrence Livermore National Laboratory. Readily available. | Total doc. | N/A | 6.8.3 | Commercial off-the-shelf software in reactor applications. | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2. Technical Product Input Source Title and Identifier(s) with Version | 3. Section | | | | | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>61 | NUREG/CR-6463 Rev. 1. 1997. *Review Guidelines for Software Languages for Use in Nuclear Power Plant Safety Systems.* Beverly Hills, California: SoHaR Incorporated. Readily available. | Total doc. | N/A | 6.8.3 | Software languages for use in nuclear power plants. | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | | | | | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| 2. Technical Product Input Source Title and Identifier(s) with Version | | 3. Section | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>62 | NUREG/CR-6465. 1996. *Development of Tools for Safety Analysis of Control Software in Advanced Reactors.* El Segundo, California: ASCA, Inc. Readily available. | Total doc. | N/A | 6.8.3 | Safety analysis of control software in advanced reactors. | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| 2. Technical Product Input Source Title and Identifier(s) with Version | | 3. Section | | | | | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>63 | Regulatory Guide 1.152 Rev. 1. 1996. *Criteria for Digital Computers in Safety Systems of Nuclear Power Plants.* Washington, D.C.: U. S. Nuclear Regulatory Commission. Readily available. | Total doc. | N/A | 6.6.2 | Digital computers in safety systems of nuclear power plants. | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| 2. Technical Product Input Source Title and Identifier(s) with Version | | 3. Section | | | | | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>64 | Regulatory Guide 1.153 Rev. 1. 1996. *Criteria for Safety Systems.* Washington, D.C.: U. S. Nuclear Regulatory Commission. Readily available. | Total doc. | N/A | 6.6.2 | Safety systems. | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | | | | | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2. Technical Product Input Source Title and Identifier(s) with Version | 3. Section | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>65 | Regulatory Guide 1.168. 1997. *Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants.* Washington, D.C.: U. S. Nuclear Regulatory Commission. Readily available. | Total doc. | N/A | 6.6.2.3, 6.8.3 | Digital computer software used in safety systems of nuclear power plants. | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | | | | | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2. Technical Product Input Source Title and Identifier(s) with Version | 3. Section | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>66 | Regulatory Guide 1.169. 1997. *Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants*. Washington, D.C.: U. S. Nuclear Regulatory Commission. Readily available. | Total doc. | N/A | 6.6.2.3, 6.8.3 | Digital computer software used in safety systems of nuclear power plants. | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2. Technical Product Input Source Title and Identifier(s) with Version | 3. Section | | | | | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>67 | Regulatory Guide 1.170. 1997. *Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants.* Washington, D.C.: U. S. Nuclear Regulatory Commission. Readily available. | Total doc. | N/A | 6.8.3 | Digital computer software used in safety systems of nuclear power plants. | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| 2. Technical Product Input Source Title and Identifier(s) with Version | | 3. Section | | | | | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>68 | Regulatory Guide 1.171. 1997. *Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants.* Washington, D.C.: U. S. Nuclear Regulatory Commission. Readily available. | Total doc. | N/A | 6.8.3 | Digital computer software used in safety systems of nuclear power plants. | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| 2. Technical Product Input Source Title and Identifier(s) with Version | | 3. Section | | | | | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>69 | Regulatory Guide 1.172. 1997. *Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants*. Washington, D.C.: U. S. Nuclear Regulatory Commission. Readily available. | Total doc. | N/A | 6.8.3 | Digital computer software used in safety systems of nuclear power plants. | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | |
|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | Change:<br>N/A | Title:<br>Subsurface Repository Integrated Control System Design |

| Input Document | | | | | | | 8. TBV Due To | | |
|---|---|---|---|---|---|---|---|---|---|
| | 2. Technical Product Input Source Title and Identifier(s) with Version | 3. Section | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>70 | Regulatory Guide 1.173. 1997. *Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants.* Washington, D.C.: U. S. Nuclear Regulatory Commission. Readily available. | Total doc. | N/A | 6.8.3 | Digital computer software used in safety systems of nuclear power plants. | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |

## OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT
## DOCUMENT INPUT REFERENCE SHEET

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1. Document Identifier No./Rev.:<br>ANL-MGR-CS-000001/REV 00 | | Change:<br>N/A | | Title:<br>Subsurface Repository Integrated Control System Design | | | | | |
| Input Document | | | | | | | 8. TBV Due To | | |
| 2. Technical Product Input Source Title and Identifier(s) with Version | | 3. Section | 4. Input Status | 5. Section Used in | 6. Input Description | 7. TBV/TBD Priority | Unqual. | From Uncontrolled Source | Un-confirmed |
| 2a<br>71 | CRWMS M&O 1999. *Development Plan*. TDP-MGR-CS-000001. Las Vegas, Nevada: CRWMS M&O ACC: MOL.19991203.0418. | Total doc. | N/A | 2. | Analysis development plan | N/A | | | |
| | | | | | | | | | |
| | | | | | | | | | |