

ANALYSIS/MODEL COVER SHEET

Complete Only Applicable Items

| | | | | | | | | | | | | | |
|---|---|---|--------------------------|---|--|--|---|---------------|---|-----------------------|--|---------------|--|
| <p>2. <input checked="" type="checkbox"/> Analysis Check all that apply</p> <table border="1" style="width:100%; border-collapse: collapse;"> <tr> <td style="width:20%;">Type of Analysis</td> <td> <input checked="" type="checkbox"/> Engineering <input type="checkbox"/> Performance Assessment <input type="checkbox"/> Scientific </td> </tr> <tr> <td>Intended Use of Analysis</td> <td> <input type="checkbox"/> Input to Calculation <input type="checkbox"/> Input to another Analysis or Model <input checked="" type="checkbox"/> Input to Technical Document </td> </tr> <tr> <td colspan="2">Describe use: Input to Waste Emplacement/Retrieval System Description Document and other System Description Documents that are Direct Inputs to the Site Recommendation Report</td> </tr> </table> | Type of Analysis | <input checked="" type="checkbox"/> Engineering <input type="checkbox"/> Performance Assessment <input type="checkbox"/> Scientific | Intended Use of Analysis | <input type="checkbox"/> Input to Calculation <input type="checkbox"/> Input to another Analysis or Model <input checked="" type="checkbox"/> Input to Technical Document | Describe use: Input to Waste Emplacement/Retrieval System Description Document and other System Description Documents that are Direct Inputs to the Site Recommendation Report | | <p>3. <input type="checkbox"/> Model Check all that apply</p> <table border="1" style="width:100%; border-collapse: collapse;"> <tr> <td style="width:20%;">Type of Model</td> <td> <input type="checkbox"/> Conceptual Model <input type="checkbox"/> Abstraction Model <input type="checkbox"/> Mathematical Model <input type="checkbox"/> System Model <input type="checkbox"/> Process Model </td> </tr> <tr> <td>Intended Use of Model</td> <td> <input type="checkbox"/> Input to Calculation <input type="checkbox"/> Input to another Model or Analysis <input type="checkbox"/> Input to Technical Document </td> </tr> <tr> <td colspan="2">Describe use:</td> </tr> </table> | Type of Model | <input type="checkbox"/> Conceptual Model <input type="checkbox"/> Abstraction Model <input type="checkbox"/> Mathematical Model <input type="checkbox"/> System Model <input type="checkbox"/> Process Model | Intended Use of Model | <input type="checkbox"/> Input to Calculation <input type="checkbox"/> Input to another Model or Analysis <input type="checkbox"/> Input to Technical Document | Describe use: | |
| Type of Analysis | <input checked="" type="checkbox"/> Engineering <input type="checkbox"/> Performance Assessment <input type="checkbox"/> Scientific | | | | | | | | | | | | |
| Intended Use of Analysis | <input type="checkbox"/> Input to Calculation <input type="checkbox"/> Input to another Analysis or Model <input checked="" type="checkbox"/> Input to Technical Document | | | | | | | | | | | | |
| Describe use: Input to Waste Emplacement/Retrieval System Description Document and other System Description Documents that are Direct Inputs to the Site Recommendation Report | | | | | | | | | | | | | |
| Type of Model | <input type="checkbox"/> Conceptual Model <input type="checkbox"/> Abstraction Model <input type="checkbox"/> Mathematical Model <input type="checkbox"/> System Model <input type="checkbox"/> Process Model | | | | | | | | | | | | |
| Intended Use of Model | <input type="checkbox"/> Input to Calculation <input type="checkbox"/> Input to another Model or Analysis <input type="checkbox"/> Input to Technical Document | | | | | | | | | | | | |
| Describe use: | | | | | | | | | | | | | |

4. Title:
Instrumentation and Controls for Waste Emplacement

5. Document Identifier (including Rev. No. and Change No., if applicable):
ANL-WES-CS-000001 REV 00 ICN 01

| | |
|--------------------------------------|---|
| 6. Total Attachments: NONE | 7. Attachment Numbers - No. of Pages in Each: N/A |
|--------------------------------------|---|

| | Printed Name | Signature | Date |
|-------------------------|------------------------|-------------------------------|-----------|
| 8. Originator | Norman T. Raczka | <i>Norman T. Raczka</i> | 7/11/2000 |
| 9. Checker | Robert Zimmerman | <i>Robert Zimmerman</i> | 7/11/2000 |
| 10. Lead/Supervisor | Bruce T. Stanley | <i>Bruce T. Stanley</i> | 7/12/2000 |
| 11. Responsible Manager | Daniel G. McKenzie III | <i>Daniel G. McKenzie III</i> | 7/12/2000 |

12. Remarks:
 The following TBXs are contained within this document:
 TBD: 406

OFFICE OF CIVILIAN RADIOACTIVE WASTE MANAGEMENT

ANALYSIS/MODEL REVISION RECORD

Complete Only Applicable Items

2. Analysis or Model Title:

Instrumentation and Controls for Waste Emplacement

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

ANL-WES-CS-000001 REV 00 ICN 01

4. Revision/Change No.

5. Description of Revision/Change

00

Initial Issue

00/01

Added Reference to CRWMS M&O 2000f (page 11); Added Statement concerning Applicability of AP-SV.1Q (page 13); Removed extra "the" in sentence (page 31); Added period to sentence (page 39); Changed reference from Section 1.0 to Section 1. (page 41); Added period before the end parenthetical mark (page 48); Added space after Orvis (page 74); Replaced URN-0149 with MOL.20000420.0399 (page 86); Added Reference CRWMS M&O 2000f (page 87); Added Reference AP-SV.1Q (page 88); Replaced Library Tracking Number L-1468 with TIC:247962 (page 88); Replaced Library Tracking Number L-1467 with TIC:247961 (page 88).

CONTENTS

| | Page |
|--|-------------|
| 1. PURPOSE | 11 |
| 2. QUALITY ASSURANCE | 13 |
| 3. COMPUTER SOFTWARE AND MODEL USAGE | 15 |
| 4. INPUTS | 17 |
| 4.1 DATA AND PARAMETERS | 17 |
| 4.2 CRITERIA | 17 |
| 4.3 CODES AND STANDARDS | 18 |
| 5. ASSUMPTIONS | 21 |
| 6. ANALYSIS | 23 |
| 6.1 INTRODUCTION | 23 |
| 6.2 WASTE EMPLACEMENT CONCEPT-OF-OPERATIONS | 23 |
| 6.3 INSTRUMENTATION & CONTROLS DESIGN FACTORS | 26 |
| 6.4 CONTROL SYSTEM FUNCTIONAL BLOCK DIAGRAMS | 31 |
| 6.4.1 Overview of Control System Functional Block Diagrams | 31 |
| 6.4.2 Functional Block Diagrams for the Waste Emplacement Control System | 39 |
| 6.5 WASTE EMPLACEMENT CONTROL & COMMUNICATION | 40 |
| 6.5.1 Emplacement Vehicle Control Systems: Background | 40 |
| 6.5.2 Emplacement Vehicle Control Systems: Preliminary Design | 41 |
| 6.5.3 Emplacement Vehicle Communication Systems: Preliminary Design | 44 |
| 6.5.4 Emplacement Vehicle Software | 45 |
| 6.6 EMPLACEMENT GANTRY | 46 |
| 6.6.1 Emplacement Gantry: Component Systems | 47 |
| 6.6.2 Preliminary Emplacement Gantry Input/Output List | 53 |
| 6.6.3 Emplacement Gantry Carrier | 54 |
| 6.6.4 Emplacement Gantry Carrier Control Interfaces | 57 |
| 6.7 TRANSPORT LOCOMOTIVE | 57 |
| 6.7.1 Transport Locomotive Control Functions | 58 |
| 6.7.2 Interfaces between Primary and Secondary Transport Locomotives | 62 |
| 6.7.3 Transport Locomotive Input/Output List | 64 |
| 6.8 WASTE PACKAGE TRANSPORTER | 65 |
| 6.8.1 Preliminary Waste Package Transporter Input/Output List | 66 |
| 6.9 WASTE EMPLACEMENT DATA COMMUNICATION | 70 |
| 6.9.1 Operator Interfaces and Control Stations | 70 |
| 6.10 SAFETY AND RELIABILITY | 72 |
| 6.10.1 Terminology and General Issues | 72 |
| 6.10.2 Waste Emplacement System Reliability, Availability, and Maintainability | 74 |

CONTENTS (Continued)

| | Page |
|--|-------------|
| 7. CONCLUSIONS..... | 79 |
| 8. REFERENCES..... | 85 |
| 8.1 DOCUMENTS CITED..... | 85 |
| 8.2 CODES, STANDARDS, REGULATIONS, AND PROCEDURES..... | 88 |
| 9. ATTACHMENTS | 91 |

FIGURES

| | Page |
|---|-------------|
| Figure 1. Waste Emplacement System Functional Block Diagram – Sheet 1 | 33 |
| Figure 2. Waste Emplacement System Functional Block Diagram – Sheet 2 | 35 |
| Figure 3. Waste Emplacement System Functional Block Diagram – Sheet 3 | 37 |
| Figure 4. Generic Mobile-Remote Control System for Emplacement Vehicles Including the Transport Locomotives and the Emplacement Gantry Design Concepts | 43 |
| Figure 5. Emplacement Gantry | 49 |
| Figure 6. Emplacement Gantry Carrier | 55 |
| Figure 7. Transport Locomotive | 59 |
| Figure 8. Control Interfaces for Locomotives in Tandem Control Configuration | 63 |
| Figure 9. Waste Package Transporter | 67 |
| Figure 10. Operations Monitoring and Control System Interfaces | 71 |

INTENTIONALLY LEFT BLANK

TABLES

| | Page |
|---|-------------|
| Table 1. System Inputs/Outputs | 18 |
| Table 2. Emplacement Concept of Operations and Control Modes..... | 24 |
| Table 3. LADS – EDA II Impact on Design of Instrumentation and Controls for Waste Emplacement..... | 27 |
| Table 4. Major Phases and Milestones for Software Development..... | 46 |
| Table 5. Emplacement Gantry Control System Input/Output List..... | 53 |
| Table 6. Emplacement Gantry Carrier Control System Input/Output List | 57 |
| Table 7. Transport Locomotive Control System Input/Output List..... | 64 |
| Table 8. Waste Package Transporter Control System Input/Output List..... | 69 |

INTENTIONALLY LEFT BLANK

ACRONYMS AND ABBREVIATIONS

ACRONYMS

| | |
|------|--|
| DBE | design basis event |
| EDA | enhanced design alternative |
| I&C | instrumentation and control |
| I/O | input/output |
| MGR | monitored geologic repository |
| MPU | microprocessing unit |
| OMCS | operations monitoring and control system |
| PLC | programmable logic controller |
| RAM | reliability, availability, and maintainability |
| SDD | system description document |
| SSC | systems, structures, and components |
| WP | waste package |

ABBREVIATIONS

| | |
|------|---------------------|
| Mbps | megabits per second |
|------|---------------------|

INTENTIONALLY LEFT BLANK

1. PURPOSE

The purpose of this analysis is to review and refine design concepts related to instrumentation, control, and remote handling systems presently under consideration for use in the waste package (WP) emplacement process at the potential subsurface nuclear waste repository at Yucca Mountain. The design concepts presented and evaluated within this analysis are based on the current system functions and criteria identified in the *Waste Emplacement/Retrieval System Description Document* (SDD) (CRWMS M&O 2000e).

This analysis focuses on the development of Instrumentation and Control (I&C) design concepts for the major elements of the waste emplacement process. It includes initial I&C designs for the Transport Locomotives, Waste Package Transporter, Emplacement Gantry, and Emplacement Gantry Carrier. Waste retrieval will be covered in a separate analysis.

This document incorporates the latest repository design changes following the Project's evaluation of a series of Enhanced Design Alternatives (EDAs) (CRWMS M&O 1999f). Significant design changes include: thermal line loading of the emplacement drifts, closer spacing of the WPs, wider spacing and fewer emplacement drifts, continuous ventilation of all active emplacement drifts, thinner walled WP designs which will increase external radiation levels, a 50-year repository closure option, inclusion of a drip-shield, backfill as an option, and new conceptual designs for the waste emplacement vehicles and equipment (CRWMS M&O 2000b, section 6, Stroupe 2000).

This analysis:

- Presents an overall I&C functional block diagram for the waste emplacement system (Section 6.4)
- Discusses and presents a general control system architecture for controlling mobile waste emplacement equipment (Section 6.5)
- Identifies specific I&C design concepts for the Transport Locomotives, Waste Package Transporter, Waste Emplacement Gantry, and Emplacement Gantry Carrier (Sections 6.6 to 6.8)
- Identifies and discusses data communication interfaces required for the waste emplacement process (Section 6.9)
- Identifies and discusses system safety and reliability issues (Section 6.10)

This design analysis has been prepared in accordance with approved development plans (CRWMS M&O 2000d, CRWMS M&O 2000f).

INTENTIONALLY LEFT BLANK

2. QUALITY ASSURANCE

The quality assurance classification of repository structures, systems, and components has been performed in accordance with QAP-2-3, *Classification of Permanent Items*. The Instrumentation and Controls for the Waste Emplacement System has been classified as quality affecting by the *Classification of the MGR Waste Emplacement System* (CRWMS M&O 1999a, page 8).

The preparation of this design analysis has been conducted in accordance with AP-3.10Q *Analyses and Models*, and has been evaluated in accordance with QAP-2-0, *Conduct of Activities*. The activity evaluation for the Waste Emplacement System (CRWMS M&O 1999c) has determined that this activity is subject to the requirements of the *Quality Assurance Requirements and Description* (DOE 2000).

The method used to control the electronic management of data as required by AP-SV.1Q, was accomplished with the controls as specified in the development plan (CRWMS M&O 2000f).

INTENTIONALLY LEFT BLANK

3. COMPUTER SOFTWARE AND MODEL USAGE

Not Applicable. The Project-standard suite of office software for word processing has been used in the preparation of this analysis. The figures have been drawn using Project-standard Computer Aided Design Drafting programs. These are commercially available software programs, that are appropriate for the application, approved for the Project, and no special qualifications are needed.

INTENTIONALLY LEFT BLANK

4. INPUTS

4.1 DATA AND PARAMETERS

- 4.1.1** The design basis WP surface dose rate is estimated to be between 200 to 400 rem/hr (CRWMS M&O 1999e, p. 25, Table 5-7). For the purposes of this analysis, the exact dose rate is not important. If the dose rate is approximately within the range cited above, this analysis and its conclusions are valid.

4.2 CRITERIA

This document is consistent with the guidance contained in the *Technical Guidance Document for License Application Preparation* (YMP 1999b). The *Revised Interim Guidance Pending Issuance of the New U.S. Nuclear Regulatory Commission (NRC) Regulations (Revision 01, July 22, 1999), for Yucca Mountain, Nevada* (Dyer 1999) is a document that was issued in anticipation of the interim guidance being promulgated as a Code of Federal Regulations. Applicable requirements associated with this interim licensing guidance, along with the *Monitored Geologic Repository Requirements Document* (YMP 1999a) are allocated to the *Waste Emplacement/Retrieval System Description Document* (CRWMS M&O 2000e, section 1.2), which in turn is the primary source of criteria and requirements for this analysis.

- 4.2.1** The waste system shall ensure that the possibility of an uncontrolled descent down the North or South Ramp of system equipment carrying a WP is limited to less than 1×10^{-6} events/year (CRWMS M&O 2000e, Criterion 1.2.2.1.1).
- 4.2.2** The structures, systems, and components (SSCs) important to safety shall be designed to permit prompt termination of operations and maintain WPs in a safe and sustainable position during an emergency (CRWMS M&O 2000e, Criterion 1.2.2.1.5).
- 4.2.3** The waste emplacement system shall be designed in accordance with the Project ALARA (as low as is reasonably achievable) program goals (TBD-406) and the applicable guidelines in "Information Relevant to Ensuring that Occupational Radiation Exposures at Nuclear Power Stations Will Be As Low As Is Reasonably Achievable" (Regulatory Guide 8.8) (CRWMS M&O 2000e, Criterion 1.2.2.1.9).
- 4.2.4** The system shall receive electrical power from the Subsurface Emplacement Transportation System (CRWMS M&O 2000e, Criterion 1.2.4.11).
- 4.2.5** The system shall receive and provide the operational information, status, and control data as outlined in the following Table 1 to the Monitored Geologic Repository (MGR) Operations Monitoring and Control System (OMCS) (CRWMS M&O 2000e, Criterion 1.2.4.13).

Table 1. System Inputs/Outputs

| Inputs | Outputs |
|--|--|
| Radiation monitoring data and status | Equipment status and status of operations |
| Subsurface Electrical Distribution System data and status monitoring | Equipment alarm status |
| Subsurface Fire Suppression System data and status monitoring | Control equipment, status, and alarms |
| WP identification and tracking data | Interlock status |
| Operational message advisory | Video signals |
| Activity plans and procedures | Communications equipment status |
| Emergency response commands | Timeout warnings for handling equipment |
| MGR operational alarm status | Control loads left in improper states (suspended loads, unattended controls, etc.) |
| Remote Control of System Equipment | Control equipment, status, and alarms |

4.2.6 The system shall include provisions for the inspection, testing, and maintenance of system equipment (CRWMS M&O 2000e, Criterion 1.2.5.1).

4.2.7 The inherent availability for the system shall be greater than 0.9485 (CRWMS M&O 2000e, Criterion 1.2.5.2).

4.3 CODES AND STANDARDS

4.3.1 Institute of Electrical and Electronics Engineers (IEEE)

| | |
|-------------------------|--|
| ANSI/IEEE Std 352-1987 | IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems (1987) |
| ANSI/IEEE Std 577-1976 | IEEE Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Power Generating Stations (1976) |
| ANSI/IEEE Std 1008-1987 | IEEE Standard for Software Unit Testing (1987) |
| IEEE Std 7-4.3.2-1993 | IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations (1993) |
| IEEE Std 379-1994 | IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems (1994) |
| IEEE Std 603-1998 | IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations (1998) |
| IEEE Std 730-1998 | IEEE Standard for Software Quality Assurance Plans (1998) |

IEEE Std 828-1998

IEEE Standard for Software Configuration Management Plans (1998)

IEEE Std 829-1998

IEEE Standard for Software Test Documentation (1998)

IEEE Std 1028-1997

IEEE Standard for Software Reviews (1997)

INTENTIONALLY LEFT BLANK

5. ASSUMPTIONS

None used.

INTENTIONALLY LEFT BLANK

6. ANALYSIS

6.1 INTRODUCTION

The primary function of the Waste Emplacement System is to transport and emplace radioactive WPs within a geologic repository with the intent of permanent storage. This document outlines the basic design concepts associated with the rail-based heavy-haul equipment needed to transport and emplace WPs within a subsurface repository. It focuses primarily on the design of instrumentation and control systems needed to implement the WP emplacement process.

A high-level strategy for the implementation of I&C systems within the potential repository is outlined in the report *Monitored Geologic Repository Instrumentation and Control System Strategy* (MGR I&C Strategy) (CRWMS M&O 1999b). The objective of the MGR I&C Strategy document is to develop an integrated and consistent process for identifying, prioritizing, and allocating I&C system requirements on a site-wide basis. It also outlines monitoring and control methods, and provides guidance on applicable codes and standards. The MGR I&C Strategy document provides a basis for the development of I&C design concepts within this analysis.

The *Subsurface Repository Integrated Control System Design* analysis (CRWMS M&O 2000a) is another document that provides a high-level framework for the design information developed within this analysis. The *Subsurface Repository Integrated Control System Design* document establishes both functional and physical control-system architectures for integrating subsurface I&C systems. These functional and physical architectures show the overall breath and scope of subsurface I&C and communication systems. They help to determine how, and on what level, subsurface systems will be monitored, controlled and interfaced.

This analysis provides a brief overview of the current concept-of-operations for the waste emplacement process in Section 6.2. In Section 6.3, several key design factors and issues related to employing digital I&C systems within a safety-conscious nuclear environment are discussed. Section 6.4 presents an overall functional block diagram for the waste emplacement system that maps the I&C-related control functions appearing in the SDD to the individual SSCs being developed to satisfy those functions. Section 6.5 presents a general control system architecture for controlling the mobile, remotely operated waste emplacement equipment. Sections 6.6 through 6.8 develop specific I&C design concepts, including preliminary instrument lists, for the Transport Locomotives, Waste Package Transporter, Emplacement Gantry, and Emplacement Gantry Carrier. Section 6.9 outlines data communication interfaces, while Section 6.10 discusses control system safety and reliability issues. General conclusions and recommendations are summarized in Section 7.0.

6.2 WASTE EMPLACEMENT CONCEPT-OF-OPERATIONS

This section provides a brief outline of the overall concept-of-operations for the waste emplacement process. It also identifies the primary control modes for each of the major operations.

The MGR I&C Strategy document (CRWMS M&O 1999b, Appendix A) provides guidance for the allocation of I&C functions within the potential subsurface repository. Systems and operations associated with transferring (i.e., transporting) WPs from surface facilities to the subsurface emplacement drifts are identified and allocated to various control and monitoring modes.

In addition, other analyses have been performed that evaluate specific activities in the emplacement process and recommend appropriate methods for monitoring and control (CRWMS M&O 1995, section 8; CRWMS M&O 1997d, sections 7.2-7.4; CRWMS M&O 1998b, section 6). Criteria such as public and occupational safety, initial and life-cycle costs, system performance and functionality, overall system reliability, availability and maintainability requirements, maturity of control technologies, regulatory and licensing precedence, etc., were considered in the development of the current control methodology. Table 2 summarizes the current consensus on the control modes for various aspects of the waste emplacement process (CRWMS M&O 1999b, Appendix A).

Table 2. Emplacement Concept of Operations and Control Modes

| Emplacement Operation | Description | Control Mode |
|---|--|--|
| WP is loaded into Transporter | At a loading bay within an air lock at the Waste Handling Building, WPs on pallets are loaded into the Waste Package Transporter coupled to a Locomotive. | Remote handling & remote monitoring from Central Control Room |
| Transporter preparation | The Transporter shielding doors are closed. The Loaded Transporter is moved outside the air lock area. | Remote operation and monitoring from Central Control Room |
| Locomotives and Transporter transport WP to subsurface | A second locomotive is coupled to the back of the Transporter and the two locomotives are used to haul the loaded Transporter from the Waste Handling Building to a subsurface area immediately outside the turnout entrance of a designated emplacement drift. | Manual control operation with real-time remote supervisory monitoring from a Central Control Room. Remote control is an option. |
| Locomotive backs Transporter into emplacement drift turnout | The rear locomotive is uncoupled and separated from the Transporter. The front Locomotive is switched to remote-control mode, the operators leave the area, all shielding doors open, and the Transporter is backed into the drift docking area. | Remote operation and monitoring from Control Room |
| Transporter prepares WP for unloading | The WP and pallet assembly is moved out onto the loading platform of the Transporter via the rigid chain guide mechanism. | Remote operation and monitoring from Control Room |
| Emplacement Gantry picks up the WP | The Emplacement Gantry, installed previously in the Emplacement Drift, moves into position over the WP and lifts the assembly off of the loading platform. | Remote operation and monitoring from Control Room |
| Locomotives and Transporter return to surface | The rigid chain mechanism is retracted, the Transporter is moved outside the turnout, all shielding doors are closed, the rear locomotive is coupled to the Transporter, the operators return, and the two locomotives haul the unloaded Transporter to the surface. | Remote operation and monitoring from Control Room. Once coupled, the locomotives are operated manually with remote monitoring and supervision. |
| Emplacement Gantry transports WP to location inside emplacement drift | The Emplacement Gantry transports the WP to a designated location inside the Emplacement Drift. Servo positioning I&C will be used to position WPs approximately 10 cm apart. | Remote operation and monitoring from Control Room |

| Emplacement Operation | Description | Control Mode |
|--|---|---|
| Emplacement Gantry emplaces WP | The Emplacement Gantry lowers WP pallet onto Emplacement Drift invert and the hoist mechanism is disengaged from the WP pallet assembly. | Remote operation and monitoring from Control Room |
| Equipment is prepared for next emplacement cycle | The Emplacement Gantry moves to a standby area near the entrance of the Emplacement Drift. The Locomotives and Transporter were returned previously to the surface to prepare for receipt of next WP. | Gantry is remotely operated from Control Room. |

Monitoring and control technologies change and improve at a rapid rate. Control methods and technologies that were impractical a few years ago are now in standard practice. Additional work in characterizing safety and performance risks and in optimizing the control strategies and methods is needed.

The document NUREG/CR-3331, *A Methodology for Allocating Nuclear Power Plant Control Functions to Human or Automatic Control* (Pulliam et al. 1983) describes a general method for allocating control functions to human or machine during nuclear power plant design. Although the Yucca Mountain Project is not a nuclear power plant, it is recommended that a similar process be engaged in the proposed repository design. The report discusses methods that should be employed during the early stages of a new system design. These methods will lead to an optimal allocation of control functions at the functional design level. Completion of this effort will have a direct impact upon the quantity of instruments and sophistication of the control system to be used for emplacing waste at Yucca Mountain.

For example, as considered in the *Subsurface Repository Remote Handling & Robotics Evaluation Report* (CRWMS M&O 1995, section 9), the emplacement process could be totally automated with little to no human involvement. It would be possible for an operator to input into a control system the WP identifier, the emplacement drift number, and the location within the emplacement drift (i.e., package number 123456789, drift 7, position 4). The control system could be designed to recognize this data and start the batch operation of transferring a WP underground. Once this input data has been verified, the rail switches would be automatically set to direct the locomotives to the appropriate drift entrance. Having received feedback that the rail switches have been correctly set, the main control system could give a command to start the locomotives. The locomotives would then travel at the designed speed, while on-board systems monitor all safety signals. Should an unsafe condition occur, the locomotives would stop and an alarm would sound at the central command console where a trained operator would evaluate the situation and commence corrective action.

In the East or West Main, near the appropriate emplacement drift, the locomotives could be programmed to begin the docking procedure. This would entail uncoupling the rear locomotive so the Transporter could appropriately dock at the entrance of the emplacement drift. The gantry would be suitably positioned within the drift, all doors would open, the transporter would dock, the WP would be released from the Transporter, the gantry would engage the WP and ultimately place it in the designated position within the emplacement drift. This is just a simplified version of the steps necessary to place the WP in a drift. Nothing in this process rules out the possibility of automation.

If the process were totally automated, additional sensors would be required to adequately inform the control system of the status of all on-going operations. Position, for example, would be a parameter that would require additional proximity sensors or limit switches so the locomotives and gantry could determine where they are in the repository. Video signals would be provided so that operators would be able to view the operation from the central command station.

In addition to the additional sensory equipment, the amount of software development for a totally automated process would be substantial. The control system would have to incorporate all of the decision-making algorithms and sequential logic involved in the process of emplacing waste. According to NUREG/CR-6278, software development efforts have usually been underestimated with respect to difficulty and are consistently under-funded (Lawrence and Persons 1994).

At the other end of the spectrum would be a process heavily dependent upon human interaction. Operators would drive the locomotives down the main drifts. The uncoupling operation would then take place, and an operator would drive the uncoupled locomotive away. The other operator would leave the locomotive coupled to the transporter and switch control of the locomotive to remote operation. From a remote location, another operator would control the docking process using joysticks and keyboard commands. This operator would depend on video signals to perform the required steps in the procedure. However, software and hard-wired interlocks would still be present within the control system to prevent unsafe operations or commands from taking place.

An operator from the same remote location, through the use of joysticks, can accomplish control of the forward-backward and raise-lower tasks that the gantry is required to perform. Sufficient information will be available to the operator so that informed decisions can be made during the emplacement of the WP.

From the above information it can be shown that the entire waste emplacement operation can be fully automated. However, testing and start-up operations with a completely automated control system may be difficult to accomplish because of the software complexity and the amount of interfaces required (see section 6.9). The recommended approach is to proceed with the I&C design based upon using primarily human interaction. As the physical efforts of moving an 85-metric ton WP become routine, the control system can be further enhanced, in phases, to completely automate the waste emplacement operation in the future.

6.3 INSTRUMENTATION & CONTROLS DESIGN FACTORS

The operating environment during waste emplacement will be unique and challenging. The working environment during emplacement will include: elevated operating temperatures, high levels of radiation, confined spaces, limited operating areas, hazardous material handling, operation of heavy equipment, and the risks associated with working underground. The design factors and conditions such as these have been preliminarily addressed in previous analyses (CRWMS M&O 1995, section 6; 1997b, section 7.2).

Current I&C design concepts reflect recent design changes in mechanical design of Waste Emplacement System components, including the Transport Locomotives, Waste Package Transporter, and Emplacement Gantry. In addition, the following table evaluates possible

impacts of changes to the repository design due to the License Application Design (LADS) effort and activities associated with selecting Enhanced Design Alternatives (EDA) (CRWMS M&O 1999f, Stroupe 2000). As shown in Table 3 below, the direct impacts on the basic control system design strategy and approach were considered to be minor.

Table 3. LADS – EDA II Impact on Design of Instrumentation and Controls for Waste Emplacement

| LADS - EDA II Design Changes | Impact On Waste Emplacement I&C |
|-------------------------------------|---|
| 1.0 Repository Capacity | Nominal impact. Repository capacity ultimately affects the overall number of waste packages to be emplaced and thereby affects equipment usage. |
| 2.0 Emplacement Drift Spacing | No effect on Waste Emplacement I&C |
| 3.0 Repository Location | No effect on Waste Emplacement I&C |
| 4.0 Emplacement Drift Diameter | No effect on Waste Emplacement I&C |
| 5.0 Ground Support | Use of steel sets and wire mesh may adversely impact radio frequency wave propagation within drifts. Should be considered in future analyses of the in-drift communication systems, particularly if a distributed antenna system concept is used. |
| 6.0 Invert Materials | No effect on Waste Emplacement I&C |
| 7.0 Backfill | N/A: not within the scope of this document |
| 8.0 Drift Loading | Nominal impact. Additional accuracy may be required of the Gantry positioning |
| 9.0 Drip Shield | N/A: If used, the drip shields are to be installed after waste emplacement is complete. |
| 10.0 Waste Package | Minor impact: Thinner walled waste packages emit higher doses of radiation. May need to increase shielding on protective enclosures for I&C. |
| 11.0 Waste Package Heat Output | Nominal impact. Increased per drift thermal loading counteracted by continuous drift ventilation. |
| 12.0 Repository Ventilation | Nominal impact on emplacement equipment. Additional air flow may aid equipment cooling systems. |
| 13.0 Repository Preclosure Period | Nominal impact on I&C design. Will impact I&C life-cycle costs. |
| 14.0 Waste Form/Fuel Cladding | N/A |
| 15.0 Areal Mass Loading | Nominal impact. Increased per drift thermal loading counteracted by continuous drift ventilation. |
| 16.0 Emplacement Drift Length | May impact in-drift communication system, particularly a Distributed RF Antenna System. Communication link has a limited communication distance. Design does not permit installation of repeaters in emplacement drift. |
| 17.0 Age of Waste | N/A |
| 18.0 Waste Stream Design Basis | N/A |
| 19.0 Surface Facility Design | N/A |
| 20.0 Off-normal Access | Nominal impact on I&C design. |
| 21.0 Pillar Temperatures | No effect on Waste Emplacement I&C |
| 22.0 Waste Package Inventory | No effect on Waste Emplacement I&C |

As indicated in the preceding section, successful operation of the waste emplacement equipment depends directly on the successful design and implementation of I&C. The technologies that permit remote monitoring and remote operations in hazardous environments are based on computerized controls and digital instrumentation. Therefore, this section focuses on design factors that relate to developing digital I&C components for safety-related systems within a nuclear environment.

It is important to note that the use of digital I&C technology does not have extensive precedence within the Nuclear Regulatory Commissions (NRCs) licensing and approval processes (CRWMS M&O 1999d, section 7.1). However, some digital I&C systems have been licensed and

approved on a case-by-case basis. Therefore, a well thought-out licensing strategy with regard to the use of digital I&C systems within the potential repository is essential. As indicated in the *Review of NRC Approved Digital Control Systems Analysis* (CRWMS M&O 1999d, sections 6.7, 6.8, and 7.1), the I&C licensing strategy would benefit from incorporating aspects of the approval and dedication process as discussed in NUREG-0800, Chapter 7, Rev 4.

The National Research Council, at the request of the Nuclear Regulatory Commission, conducted a study of the use of digital I&C systems in nuclear power plants (National Research Council 1997). In the report, *Digital Instrumentation and Control Systems in Nuclear Power Plants, Safety and Reliability Issues*, the National Research Council points out that the control systems in use today throughout the U.S. commercial nuclear power industry were largely designed and implemented during the era of *analog* controls, and that the introduction and acceptance of more modern *digital* control systems has been a slow and challenging process.

There are several important advantages in the use of digital I&C systems which are causing the nuclear power industry to transition away from the use of analog systems. These advantages include: (1) digital electronics are essentially free of the drift that affects analog electronics; (2) digital electronics improve system performance, accuracy, and computational capabilities; (3) they facilitate better data handling, processing, and storage; (4) digital controls are easier and more flexible to design and implement; (5) digital electronics are easier to calibrate and maintain. Since there has been a wholesale shift to digital systems in virtually all other commercial sectors, digital systems are more widely available and implemented, which is resulting in component obsolescence and waning vendor support for analog systems. Also, digital systems provide the potential for improved system capabilities such as trend monitoring, fault tolerance, self-testing, signal validation, process diagnostics, and improved human/machine interfaces. All of these reasons support the reliance on modern digital control systems in the design and development of a nuclear waste repository.

The National Research Council's report identified six technical areas and two strategic/programmatic issues that are key to the successful implementation of digital control systems within nuclear applications. The technical issues identified are:

- Systems Aspects of Digital I&C
- Software Quality Assurance
- Common-Mode Software Failure Potential
- Safety and Reliability Assessment Methods
- Human Factors and Human/Machine Interfaces
- Dedication of Commercial Off-the-Shelf Hardware and Software

The strategic/programmatic issues are:

- A Case-by-Case Licensing Process of Digital I&C
- Adequacy of the Nuclear Regulatory Commission's Technical Infrastructure

All eight of these issues are important to consider in the design and development of the waste emplacement control systems. The first six issues identified above fall generally within the

scope of this analysis and four of these are preliminarily discussed below. The four remaining issues should be addressed in future design analyses.

Systems Aspects of Digital I&C—Although the use of digital I&C technology provides important new benefits, it also could potentially introduce new failure modes. The “System Aspects” of a digital design go beyond component-level reliability issues and relate to issues such as overall system architecture, system-wide communication and protocols, allocation of functions, and real-time and distributed processing. Modern digital I&C technology lends itself to large-scale, fully integrated, multi-level control systems that can become quite extensive and complex, and it is absolutely crucial that the systems aspects of the design be adequately addressed, designed, and tested before implementation is completed.

In addition to the emplacement I&C functions identified within this analysis, there are other repository systems that will also be integrated and controlled at various levels according to the *Subsurface Repository Integrated Control System Design* analysis (CRWMS M&O 2000a, section 6.2.2). These include: surface waste handling system, subsurface ventilation system, subsurface transportation system, power distribution system, repository environmental (temperature, humidity) monitoring, radiation monitoring systems, fire detection and suppression systems, personnel and process monitoring systems, emergency response, security and access control systems, warning and alarm systems. It is clear that an integrated control system of this magnitude will require careful attention to the overall systems aspects of the design. This analysis provides preliminary design concepts related to the emplacement system control architecture, data communication, and distributed processing.

Software Quality Assurance—An important element of the design, not encountered in the older analog technology, is the use and reliance on software within the system. Digital I&C systems rely on software programs to provide important aspects of system functionality. Assuring the quality of the software is not a trivial matter. Extensive software quality assurance measures are taken in other safety-critical industries that currently rely on digital-based I&C systems. Much can be garnered from successful approaches that have been applied in safety-critical fields such as aviation, aerospace, public transit, modern chemical processing, and fossil-fuel power plants (CRWMS M&O 1998a, section 7).

Based on the QARD (DOE 2000, Supplement I), the Project has implemented key procedures to control the use and development of engineering and scientific software for design and analysis activities. Current quality assurance procedures include software verification and validation and software configuration management processes.

The process of designing reliable, high-quality real-time control software for the Waste Emplacement System may require years of development and testing. Initially, software development activities should focus on developing high-level planning documents that outline the overall development, management, testing, and product quality-assurance strategies. These planning documents should include guidance on topics such as: software design and development methodologies, application of software standards and protocols, management and control of the software development processes, work implementation plans, and overall design architectures. There will also need to be a series of analyses that identify the functional

requirements of the control software and develop preliminary designs. The issues of software quality assurance and software development are not addressed extensively within the scope of this analysis, but will be the focus of later analyses.

Common-Mode Software and Equipment Failure Potential—Computer-based control systems are becoming faster and more powerful, which allows individual processors to multiplex many diverse tasks simultaneously. While providing many benefits, this also creates areas of design concern.

Common-mode failures are failures in which a single error or problem disables multiple, independent system functions. An example of this might be the failure or loss of a key control computer or programmable logic controller (PLC) that, in turn, may render multiple other systems inoperable. Several design approaches are commonly used to minimize the possibility of this occurring in safety-critical control systems. Defense-in-depth design strategies include: use of redundant systems, use of diverse technologies and systems, physical separation of redundant or backup systems, and incorporation of fault-tolerant design features.

As indicated throughout this analysis, defense-in-depth design approaches are used when the potential consequences or costs of a failure would be considered unacceptable. Section 6.10 of this analysis provides an initial discussion of reliability, availability, and maintenance; however, additional analyses on these issues are necessary. There are a number of standards available, such as IEEE Std 379-1994, *IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems* and similar standards, developed for use in the nuclear industry, that may provide guidance in assessing the single-failure criterion.

Dedication of Commercial Off-the-Shelf Hardware and Software—As indicated in *Digital Instrumentation and Control Systems in Nuclear Power Plants, Safety and Reliability Issues* (National Research Council 1997, chapter 8), the use of commercial off-the-shelf hardware and software is attractive only if a suitable and cost-effective process can be formulated for the technology's dedication (i.e., approval and acceptance) by the NRC. It could be that the proof-testing and dedication process required by the NRC might negate the cost advantages of using commercial off-the-shelf products, and is an important point to consider in the development of digital I&C systems for the emplacement process.

The current design approach has been to survey available commercial technologies and determine how they may be applied to satisfy repository design requirements. The underlying philosophy has been that a dedication and approval process could be provided that would maintain the cost-efficiency incentives of using commercial off-the-shelf component technologies.

NRC Addressing I&C Design Issues—In recent years, the NRC has begun to address the issues related to the use of digital instrumentation, computer controls, and data communications systems within the commercial nuclear industry. The NRC has sponsored the development of several NUREGs that provide guidance for meeting regulatory requirements such as those contained in the Code of Federal Regulations (NUREG/CR-6278 (Lawrence and Persons 1994), NUREG/CR-6294 (Lawrence and Preckshot 1994), NUREG/CR-6421 (Preckshot and Scott

1996), and NUREG/CR-6082 (Preckshot 1993)). Often, the NUREGs identify or incorporate national codes and standards developed by professional societies and standardizing bodies.

It is recommended that criteria contained in the *Waste Emplacement/Retrieval System Description Document* (CRWMS M&O 2000e, section 1.2) be revised and expanded to cover I&C requirements. In this current SDD, there are references to steel, welds, and mechanical loads but virtually no mention of control communication, computers, software, instruments, sensors or human-machine interfaces. The Waste Emplacement and Retrieval Systems will be composed of on-board computers, radios, power supplies, instruments and sensors. The addition of a function similar to the following statement is suggested: “The Waste Emplacement System shall provide features for monitoring external environmental and operating conditions including visual, thermal and radiological conditions.” Note that this is a separate functional need than either Function 1.1.11 or 1.1.14. The system not only needs to “operate” within the natural and induced environmental condition but it also needs to monitor and report what those conditions are. Also, add corresponding criteria related to visual, thermal and radiological monitoring the System Design Criteria section of the SDD. A criterion should also be added to provide design engineers guidance on the system reliability requirements.

6.4 CONTROL SYSTEM FUNCTIONAL BLOCK DIAGRAMS

This section presents a preliminary functional architecture for the I&C system associated with the Waste Emplacement System. It presents a series of three control-system functional block diagrams that correlate key functions identified in the SDD to specific equipment and components being designed by the Repository Subsurface Design Group. In essence, the functional block diagrams map the I&C-related control functions appearing in the SDD to the individual SSCs being developed to satisfy those functions.

The Waste Emplacement System is one of more than 20 major systems that will be integrated within the subsurface repository design (CRWMS M&O 2000a, section 6.2.2). Preliminary functional block diagrams for the Waste Emplacement System are graphically represented in Figures 1, 2, and 3. The functional diagrams presented here have been enhanced and vary slightly from those presented in *Subsurface Repository Integrated Control System Design* (CRWMS M&O 2000a, section 6.2.3).

6.4.1 Overview of Control System Functional Block Diagrams

The functional block diagrams presented in this section depict an eight-level vertical hierarchy of I&C-related SSCs located throughout the potential 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 the control system for Waste Emplacement SSCs.

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 the SDD systems that have a functional range extending throughout the MGR. These site-wide SDDs encompass both surface and subsurface functions and operations. The Waste Emplacement and Retrieval SDD interfaces primarily with the subsurface portion of the MGR OMCS.

The “Facility Level” identifies systems whose I&C-related functions impact the subsurface facility as a whole and interface directly with site-level SDD systems. 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” indicates the SDD system that is the focus of this conceptual design analysis, namely, the Waste Emplacement System. Key I&C related functions for the system are represented on the primary function level below.

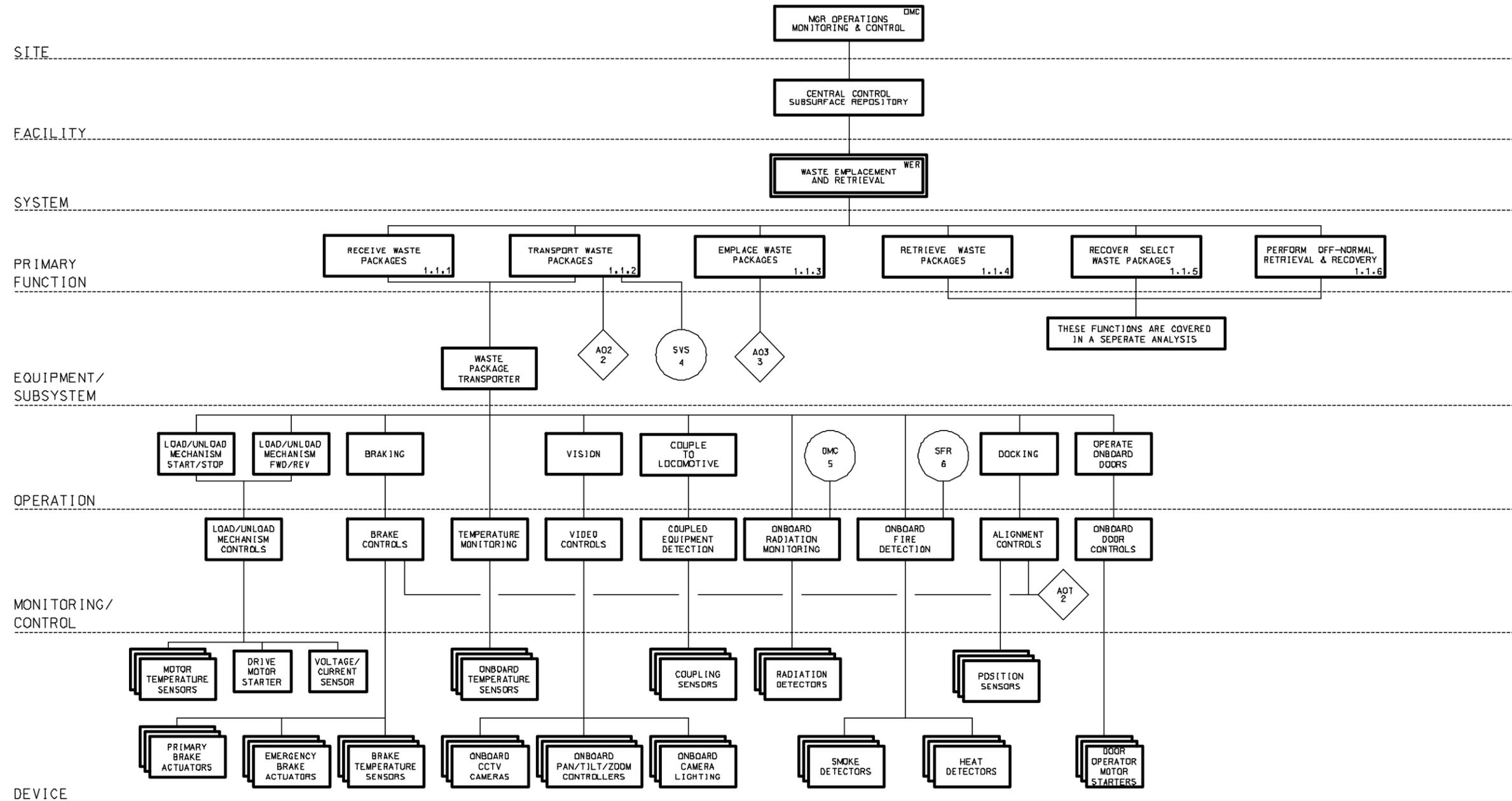
The “Primary Function Level” contains the main or primary I&C-related functions allocated to the Waste Emplacement System. These items are taken directly from the “System Functions” section of the SDD (CRWMS M&O 2000e, section 1.1). The SDD subsection number for each function appears in the lower right-hand corner of the block element. Not all functions identified in the SDD are depicted in the functional block diagrams. Only the primary functions logically related to the waste emplacement control system are considered in this analysis.

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. 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 I&C and communications related 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.



LEGEND:

FIGURE INTERCONNECTION POINT
 CONTINUATION IDENTIFIER NO.
 FIGURE NO.

SYSTEM INTERFACE POINTS
 SDD IDENTIFIER NO.
 NOTE NO.

NOTES:

1. DOUBLE BOXES INDICATE PRIMARY SYSTEM DEPICTED IN THIS FIGURE.
2. STACKED BOXES INDICATE MULTIPLE DEVICES/SYSTEMS
3. S/S - SUBSURFACE
4. SUBSURFACE VENTILATION SYSTEM (SVS)
5. MGR OPERATIONS MONITORING AND CONTROL SYSTEM (OMC)
6. SUBSURFACE FIRE PROTECTION SYSTEM (SFR)
7. POWER SYSTEM INTERFACE NOT SHOWN.

CAD FILE: cs0125.dgn

Figure 1. Waste Emplacement System Functional Block Diagram – Sheet 1

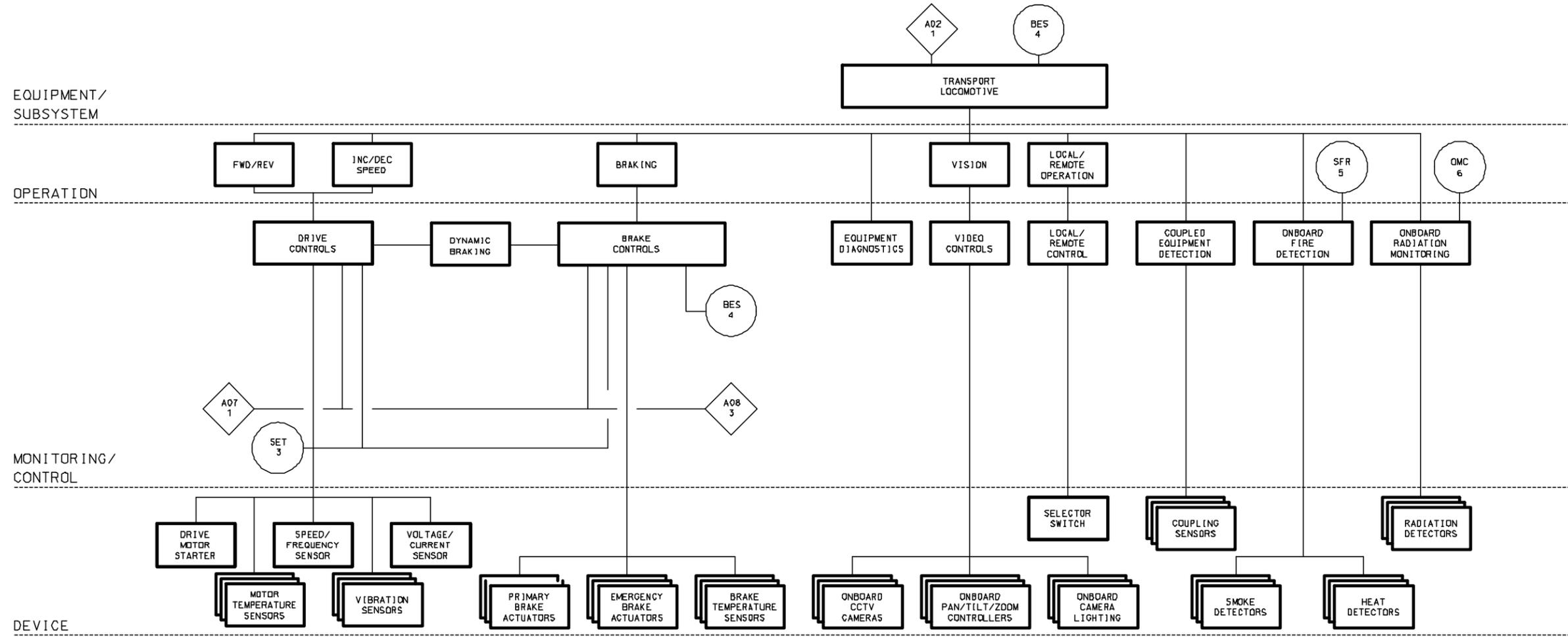
INTENTIONALLY LEFT BLANK

SITE _____

FACILITY _____

SYSTEM _____

PRIMARY FUNCTION _____



CAD FILE# es0126.dgn

LEGEND:

FIGURE INTERCONNECTION POINT
 CONTINUATION IDENTIFIER NO.
 XXX
 X
 FIGURE NO.

SYSTEM INTERFACE POINTS
 SDD IDENTIFIER NO.
 XXX
 X
 NOTE NO.

NOTES:

1. STACKED BOXES INDICATE MULTIPLE DEVICES/SYSTEMS
2. S/S - SUBSURFACE
3. SUBSURFACE EMPLACEMENT TRANSPORTATION SYSTEM (SET)
4. BACKFILL EMPLACEMENT SYSTEM (BES)
5. SUBSURFACE FIRE PROTECTION SYSTEM (SFR)
6. MGR OPERATIONS MONITORING AND CONTROL SYSTEM (OMC)

Figure 2. Waste Emplacement System Functional Block Diagram – Sheet 2

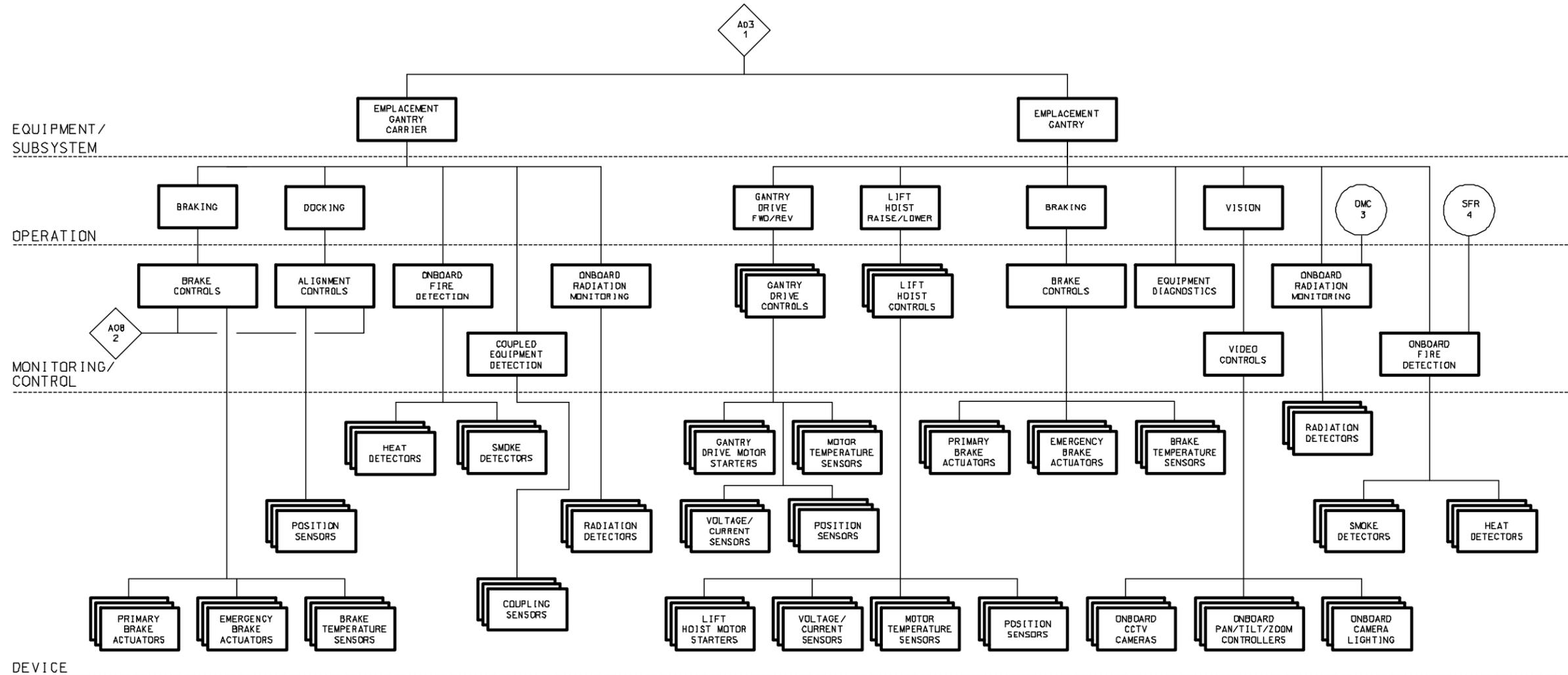
INTENTIONALLY LEFT BLANK

SITE _____

FACILITY _____

SYSTEM _____

PRIMARY FUNCTION _____



DEVICE _____

LEGEND:

FIGURE INTERCONNECTION POINT

xxx CONTINUATION IDENTIFIER NO.

x FIGURE NO.

SYSTEM INTERFACE POINTS

xxx SDD IDENTIFIER NO.

x NOTE NO.

NOTES:

1. STACKED BOXES INDICATE MULTIPLE DEVICES/SYSTEMS
2. S/S - SUBSURFACE
3. MGR OPERATIONS MONITORING AND CONTROL SYSTEM (DMC)
4. SUBSURFACE FIRE PROTECTION SYSTEM (SFR)

CAD FILE: cae0127.dgn

Figure 3. Waste Emplacement System Functional Block Diagram – Sheet 3

INTENTIONALLY LEFT BLANK

The diamond-shaped icons indicate interconnection points between the various components within the Waste Emplacement System. The circle-shaped icons indicate interface points external to the Waste Emplacement System.

6.4.2 Functional Block Diagrams for the Waste Emplacement Control System

This section presents a series of three diagrams that depict a functional architecture for the waste emplacement process (see Figures 1, 2, and 3). These functional block diagrams provide a top-down design perspective that maps each of the waste emplacement functions to the individual components and devices tasked with accomplishing those functions. The diagrams also identify key system interface points to other repository systems external to the Waste Emplacement System.

A diagram showing the high-level interfaces between the Waste Emplacement System and the MGR OMCS is provided in Figure 1. The nature of that interface is to provide supervisory monitoring and control of the entire waste emplacement process. This monitoring and control will be performed by human operators seated at control consoles located in a centralized control room that is part of the OMC system.

Figure 1 also provides the top-down functional architecture for the Waste Package Transporter. As indicated in the diagram, the Transporter will be used to receive WPs from the Waste Handling Building and in the transportation of those WPs into the subsurface repository (CRWMS M&O 2000e, section 1.1). The Waste Package Transporter will need to provide a means for loading and unloading the WPs, opening and closing shielding doors, monitoring internal temperatures and radiation levels, remotely viewing handling operations, and provide feedback and control of Transporter docking operations. The lower tiers of the functional block diagram depict the I&C devices that would implement this functionality.

Figure 2 provides a functional block diagram of the Transport Locomotive. The control system design concepts being developed for the Transport Locomotive and the Waste Emplacement Gantry (on Figure 3) include: on-board power distribution, communications, locomotion, actuators, and a variety of on-board sensors and instrumentation that will monitor vehicle performance and operating environment conditions.

The functions of either the locomotive or gantry vehicle controller include receiving high-level commands from remote operators via the communication system, converting these commands into appropriate vehicle control signals, issuing these control signals to the relevant vehicle systems, monitoring internal vehicle performance and status, and, in real-time, reporting this information back to the remote operators. The vehicle controller will monitor, control, and report on all aspects of the vehicle performance including: vehicle position, speed, direction, and acceleration; vehicle braking system status; vehicle proximity to other SSCs; overall vehicle power consumption status, as well as current draw at individual drive motors; temperatures and radiation levels at various locations within the vehicle and external to the vehicle; switching and control of the vehicle's camera systems, pan/tilt drive units, and lighting; and the operational status of all on-board actuators and instrumentation.

In addition to providing a functional block diagram of the Emplacement Gantry, Figure 3 also provides a functional block diagram of the Gantry Carrier, with corresponding interfaces identified.

6.5 WASTE EMPLACEMENT CONTROL & COMMUNICATION

This section presents preliminary design concepts for a physical architecture for controlling and communicating with the remotely-operated emplacement vehicles.

The Waste Emplacement System concept calls for the use of rail-based heavy-haul vehicles that can be manually and/or remotely operated and controlled. The primary and secondary Transport Locomotives will be capable of both manual and remote operation. The Emplacement Gantry will be strictly remotely operated and controlled. Although the basic requirements and the functionality and environmental constraints of the locomotive and gantry systems differ, it will be advantageous for these vehicles to share some common technologies and systems, such as similar control system architectures, and common methods of mobile communication. Other commonalities may also include common vehicle instrumentation, sensors, vision systems, on-board power distributions systems, and vehicle power source supply (CRWMS M&O 1999b, section 5.3).

The use of common components will help to save on overall system development costs by utilizing design efforts and reliability testing that are applicable in multiple areas within the potential repository system. It will also help to reduce maintenance and repair costs by standardizing common components where possible. This section presents preliminary designs for systems that will be common to the mobile vehicle fleet: specifically, the vehicle control system and the mobile communication system.

6.5.1 Emplacement Vehicle Control Systems: Background

This section presents design concepts for the on-board device and primary control layers associated with the design of remotely operated mobile equipment. As mentioned previously, there are advantages to employing a common control system architecture within the emplacement vehicle fleet designs being developed. This section presents a generic, on-board, vehicle control system that can serve as the basis for controlling either the emplacement locomotives or gantry systems.

In recent years, there have been significant work and accomplishments in the area of developing remotely operated vehicle technologies. As part of recent work on the Yucca Mountain Project, a series of technology surveys were conducted that identified hundreds of remotely operated vehicles that have been developed for research and for use in hazardous environments on land, in the sea, and in the air (CRWMS M&O 1995, Appendix B; 1996c). Mobile, remotely controlled equipment is being used in the mining, mass-transit, nuclear, aerospace, defense, manufacturing, and plant protection industries. The survey found that advanced vehicle control technologies are readily available and, with sufficient design engineering, testing, and evaluation, could be adapted for use in the unique environment and applications of the potential repository. As indicated in the survey, several vendors have produced remotely operated vehicles and control

components that are designed specifically for nuclear incident monitoring and mitigation (CRWMS M&O 1997b, page 43; 1996c, page IV-276).

The remote control architectures reviewed in the survey ranged in functionality, complexity, and sophistication from basic PLC technology to systems employing multiple, distributed, embedded microcontrollers, or microprocessing units (MPUs) utilizing real-time operating systems. The technologies are related in that PLCs contain very basic MPUs that have been developed to interface with and control industrial device-level analog and discrete inputs and outputs (I/O).

A fundamental difference between PLCs and MPUs is that PLCs typically excel at sequential control processes, while MPUs provide more multitasking and asynchronous control capabilities. PLCs were developed by the industrial process-control industry and were designed to operate reliably in relatively harsh environments. Although PLC technology was initially developed to control basic industrial device-level I/O, it has evolved to interface with more advanced factory functions such as motor control. The microcontrollers and MPUs that are currently being used in factory automation and industrial controls grew out of the advanced computing industry.

Another key difference between the technologies is that PLCs employ a ladder-logic software programming environment, while microcontrollers and MPUs typically provide more programming resources and richer programming environments. Microcontrollers and MPUs operate with machine code or assembly languages that are compiled from a variety of high-level programming languages. They also utilize real-time operating systems that provide interfaces to low-level devices and multitasking capabilities not typically found in PLC technology.

For the purpose of developing a design concept for site recommendation, the initial Waste Emplacement System control concepts will investigate a basic control architecture that is implemented with the simplicity of commercial PLC technology and augmented by auxiliary distributed MPUs. Future design work should investigate the advantages and disadvantages of the various vehicle-control design options and evaluate alternative control architectures, e.g., architectures that are based primarily on distributed MPU technology. Future design work will also need to address considerations for supportability, incorporating technological up-grades, and avoiding obsolescence.

6.5.2 Emplacement Vehicle Control Systems: Preliminary Design

The basic design goal is to develop high-quality emplacement vehicles that perform their intended functions in a safe and exceptionally reliable manner over the entire range of possible operating conditions. The vehicle control system is a vital element in the accomplishment of this goal.

The control systems for emplacement vehicles will also need to be reliable and robust. There are certain emplacement operations and activities that are critical and need to be reliably and successfully performed. For example, if not adequately designed, a failure in the Emplacement Gantry control system could result in the vehicle becoming disabled within an emplacement drift. However, the adverse consequences of this situation, and the anticipated cost in time and money to rectify the problem, provide ample motivation to ensure that the Emplacement Gantry control system is designed to be both robust and reliable. As indicated in Sections 1. and 6.10,

a detail treatment of issues related to failure modes or design basis events (DBEs) and their associated recovery operations are outside the scope of this analysis.

The mobile emplacement vehicles will be required to operate in an environment where ambient temperatures may reach 50 °C and radiation levels at the surface of the WPs may exceed 200 rad/hr (Design Input 4.1.1). The systems will operate primarily in the underground repository environment, but will also need to function in above-ground conditions, which would include: sunlight, wind, dust, rain, snow, and hot and cold temperatures.

For the reasons outlined in Section 6.3 (and in CRWMS M&O 1997a, Section 7.4), availability and maturity of commercial technology, design reliability and robustness, design precedence in mobile remote systems already approved by the NRC, and the overall relative simplicity of emplacement vehicle control functions, this initial design effort will consider a PLC-based vehicle control system augmented by microcontroller or MPU-based systems (see Figure 4). Later analyses can examine alternative vehicle control systems that are based directly on distributed microcontroller and MPU-based control architectures.

The design effort focuses on making key vehicle systems reliable. Every effort will go toward preventing, or minimizing, the likelihood of even low-probability malfunctions within key vehicle systems.

Some types of failures are more tolerable than others. For example, if a malfunction should cause the Transport Locomotive to lose contact with the power or communication systems, fail-safe brakes would engage and the locomotive would come to a controlled stop. This is considered failing in a safe or graceful manner. While this scenario is undesirable, it would not be dangerous nor difficult to recover from. The locomotive could be disengaged and towed to the surface for repairs and an auxiliary or backup locomotive could be brought in to continue operations. Other malfunctions, however, may not be so tolerable. For example, failure of the braking system, or run-away vehicle conditions, would be dangerous situations that could cause considerable damage or injury. Because the consequences are so severe, much of the design effort is focused on ensuring that these types of malfunctions do not occur at all. Redundancy will be incorporated in the design and other design analyses will be completed to evaluate this type of failure, should it occur.

There are several design strategies and design tools that are commonly used to ensure that key systems are designed to be exceptionally safe, dependable, and reliable. These include the following: employing defense-in-depth strategies; use of high-quality components that are developed under stringent quality control and certification procedures; use of redundant systems; use of backup systems; use of diverse technologies and systems; physical separation of redundant or backup systems; extensive design prototyping; and a program of rigorous and extensive reliability and environmental testing of final designs. The emplacement vehicle control system is a key system that will employ these design techniques.

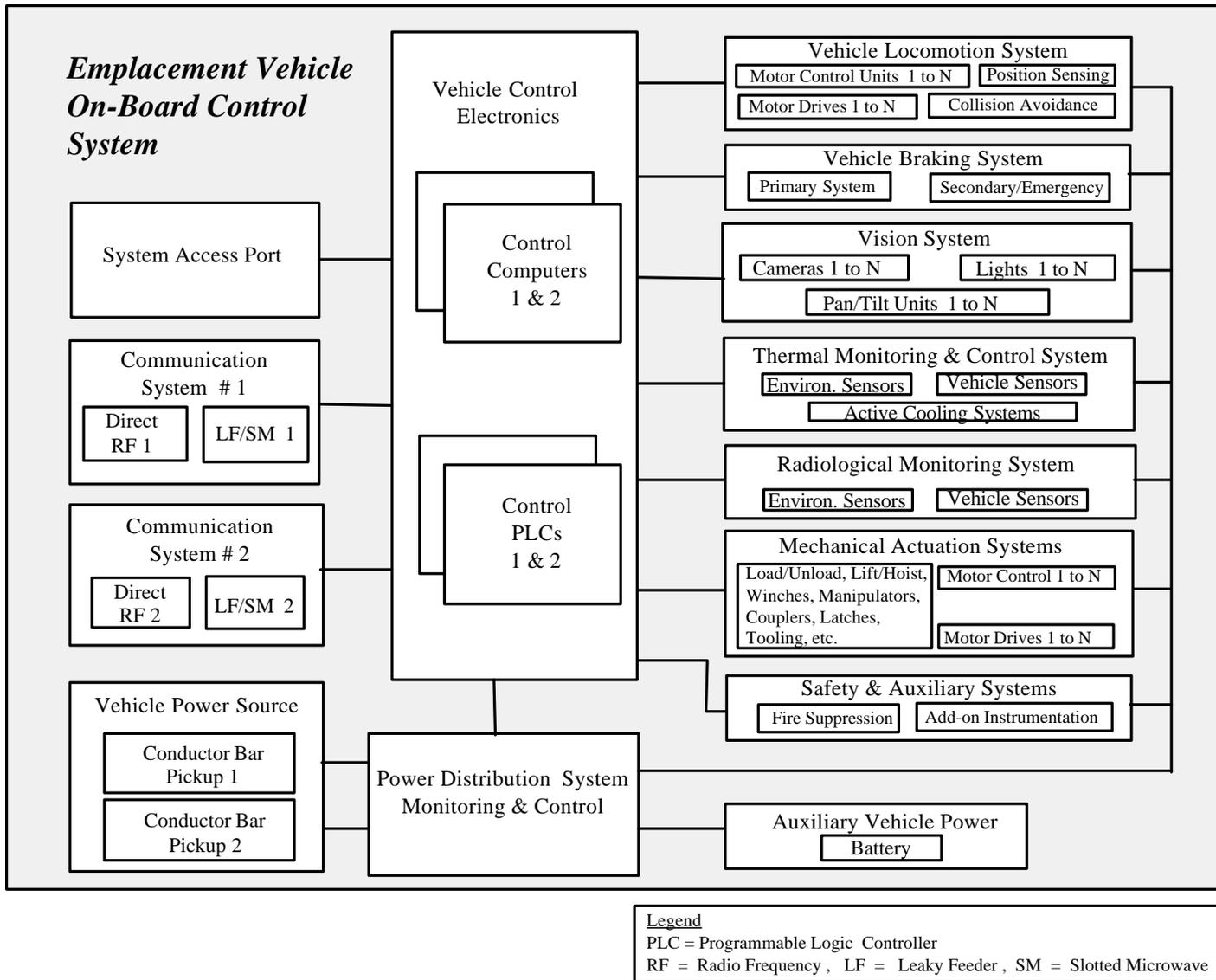


Figure 4. Generic Mobile-Remote Control System for Emplacement Vehicles Including the Transport Locomotives and the Emplacement Gantry Design Concepts

As shown in Figure 4, the initial design of a basic emplacement vehicle control system can be based on a redundant, fault tolerant, PLC-based configuration. The redundant PLCs could be designed to operate in parallel and employ an I/O voting strategy, where both PLCs would have to agree before implementing a command or confirming a condition. Another implementation approach would be to configure one of the PLCs as the active primary system, with the second PLC serving as hot-swappable backup on standby.

There are other levels of system redundancy available in the way software systems are programmed. For example, software can be developed in such a way that each PLC does not implement identical software code that could present the possibility of common failure modes. Additional levels of reliability can be added by incorporating software checking routines that verify data/command integrity. The reliability of the control system design can also be enhanced by configuring critical system I/O devices using fault tolerant strategies, and by locating control units on physically separate sides of the vehicle.

Additional vehicle reliability support could be provided by two on-board auxiliary MPUs. The MPUs add an element of control diversity and could be programmed to monitor and forecast vehicle performance trends, warn operators when system performance limits are approached, perform on-board diagnostics, and provide emergency backup recovery routines.

Therefore, the basic control architecture will be founded on well-proven, relatively simple, commercially available, robust control technologies that can be implemented with several layers of functional and physical redundancies.

6.5.3 Emplacement Vehicle Communication Systems: Preliminary Design

In addition to the Transport Locomotive and Emplacement Gantry utilizing common vehicle control system architectures, it may also be useful to utilize similar mobile-remote communications technologies. The use of common communication technologies will help save on overall system development costs by utilizing design efforts and reliability testing that are applicable in multiple areas within the potential repository system. It will also help to reduce maintenance and repair costs by standardizing common components where possible.

The *Subsurface Waste Package Handling - Remote Control and Data Communications Analysis* (CRWMS M&O 1997d, section 7.4.2) examined several alternative technologies for mobile-remote communication. These included: distributed antenna-direct radio systems, leaky feeder coax cable antenna systems for near-field radio control, slotted microwave guide transmission technology like that used in rail-transit systems, standard microwave communications systems (without the use of waveguides), laser/optical systems, infrared systems, tethered cable-reel systems, festoon cable management systems, and electrified conductor bar systems. For reasons indicated within the referenced analysis, the direct radio, leaky feeder, and slotted microwave technologies are being considered for use in subsurface communication in the potential repository.

Due to the critical need for developing an exceptionally reliable communication system, the current design approach will be to implement redundant communication systems on each mobile emplacement vehicle. In addition, it is planned to use two of the three communication

technologies recommended above in order to further ensure communication reliability by using diverse technologies, thereby reducing the chance of common-mode failures. Each mobile emplacement vehicle will be able to communicate over two totally separate and diverse communication mediums.

Even without going to the extent of incorporating redundant communication systems, many modern safety-critical applications utilize wireless mobile equipment communication technologies. For more than thirty years, crane companies have been using radio technologies to remotely control overhead gantry cranes and, more recently, construction cranes. Well-established and well-proven command and control safety-interlocks essentially eliminate the possibility of errant or corrupted commands caused by interference or equipment failure (CRWMS M&O 1998a, section 7.3.3; 1996b, page III-40; 1997d, section 7.4.1).

6.5.4 Emplacement Vehicle Software

According to NUREG/CR-6278, system software development and testing is one of the most important elements of a successful system design and one that is almost universally underestimated or overlooked in the course of system development (Lawrence and Persons 1994). Developing quality software is vital to system reliability and is a critical element of the design.

The vehicle control systems will rely on software programs to provide many of the important aspects of the system functionality. Future design work will need to adequately address the significant quantity of software that will eventually be developed to control and monitor the potential repository. Integrated software development programs typically address such things as: development methodology, development controls, product assurance and testing, QA controls, regulatory approval processes, life-cycle operations, and maintenance.

Extensive software quality assurance measures are taken in other safety-critical industries that currently rely on digitally-based I&C systems (CRWMS M&O 1998a, section 7). Much can be learned from successful approaches that have been applied in other safety-critical fields e.g., aviation, aerospace, public transit, modern chemical processing, and fossil-fuel power plants. It is recommended that preliminary software design be initiated and the functional flow diagrams be produced. This would include researching and recommending (1) possible development platforms and tools, (2) real-time operating systems, (3) real-time control issues, (4) appropriate programming languages, (5) relevant routines for error-checking, and (6) reliability and testing strategies.

Software planning and development within the context of safety-critical systems takes on an added dimension in terms of strategic features and requirements. As outlined in the *Subsurface Repository Integrated Control System Design* analysis (CRWMS M&O 2000a, section 6.8.1), Table 4 provides a chronological list of development phases and milestone reviews that could be used to model the software development process for the Waste Emplacement System.

Table 4. Major Phases and Milestones for Software Development

| Order | Phases | Milestone Reviews |
|-------|---|---|
| 1 | System Requirements Analysis | <ul style="list-style-type: none"> • Define System Functional Requirements • Establish System Management Plan |
| 2 | System Functional Design | <ul style="list-style-type: none"> • System Functional Design • Subsystem Work Implementation Plan |
| 3 | Subsystem Software Requirements Analysis | <ul style="list-style-type: none"> • Software Requirements |
| 4 | Subsystem Software Functional Design | <ul style="list-style-type: none"> • Subsystem Functional Design • Software Work Implementation Plan |
| 5 | Software Requirements Analysis | <ul style="list-style-type: none"> • Software Requirements |
| 6 | Software Design | <ul style="list-style-type: none"> • Software Design |
| 7 | Software Implementation and Testing | <ul style="list-style-type: none"> • Implementation Status • Software Delivery |
| 8 | Subsystem Integration, Test, and Delivery | <ul style="list-style-type: none"> • Subsystem Delivery |
| 9 | System Implementation, Test, and Delivery | <ul style="list-style-type: none"> • System Delivery |
| 10 | Operation and Maintenance | Covered in additional planning documents |

Inasmuch as the software-based monitoring and control functions performed by the Waste Emplacement System will take place in a nuclear environment, it is recommended that the following standards and regulations governing the use of software in the control systems of commercial nuclear power generating stations be evaluated. Such an examination and study would assist in determining the specific software planning, development, and design requirements for the Waste Emplacement System. Therefore, it is recommended that a number of IEEE standards pertaining to software development be consulted in order to establish these requirements for the Waste Emplacement System. These standards include IEEE Std 730-1998 *IEEE Standard for Software Quality Assurance Plans*, IEEE Std 828-1998 *IEEE Standard for Software Configuration Management Plans*, IEEE Std 829-1998 *IEEE Standard for Software Test Documentation*, IEEE Std 1008-1987 *IEEE Standard for Software Unit Testing*, and IEEE Std 1028-1997 *IEEE Standard for Software Reviews and Audits*.

Upon finalization of the compliance program guidance packages for the Yucca Mountain Project, all or some of these regulations and standards may be used to define the Project design criteria and requirements for the Waste Emplacement System. Although these regulatory documents apply to the commercial nuclear power industry, it is likely that some portions of their content will be applicable.

6.6 EMPLACEMENT GANTRY

In the current emplacement concept, the Emplacement Gantry is one of the most critical elements of the overall design. It is essential that this system perform its intended functions in a safe and reliable manner. The Emplacement Gantry will be designed to operate in the relatively harsh thermal and radiation environment located inside the emplacement drifts. Due to these harsh conditions, the gantry will be remotely controlled by human operators located at a remote control station. The basic purpose of the Emplacement Gantry is to transport the WPs from the

emplacement drift dock area, down the length of the emplacement drift, and place them within the drift. Since personnel will not be permitted inside the emplacement drifts under normal operating conditions, the design goal will be to design the Emplacement Gantry to perform its tasks with the utmost reliability.

As the design of the Emplacement Gantry progresses, several design approaches have and will be used to maximize system reliability and robustness. These include: use of rigorous quality control and product assurance standards throughout the system design and development processes; use of high quality components; use of redundant systems; use of backup systems; use of diverse technologies and systems; and physical separation of redundant or backup systems. These design approaches will be utilized where the potential consequences or costs of a system or component failure are considered unacceptable. Using these approaches will also result in a system with a high degree of fault tolerance.

The reliability of the Emplacement Gantry is further enhanced because the vehicle will be highly accessible for periodic maintenance. The concept of operations calls for the gantry to be frequently removed from the emplacement drifts, thereby providing personnel with direct access to the equipment for preventative and/or corrective maintenance.

A preliminary design of the mechanical and structural elements of the Emplacement Gantry was presented recently in the analysis *Bottom/Side Lift Gantry Conceptual Design* (CRWMS M&O 2000c). The basic mechanical configuration of the Emplacement Gantry is shown in Figure 5. The purpose of the following sections is to describe the basic control elements of the Emplacement Gantry.

6.6.1 Emplacement Gantry: Component Systems

The Emplacement Gantry design is made up of several major systems, which include: the mechanical structure, an on-board control system, power supply and distribution systems, communication systems, vehicle locomotion and braking systems, lifting head and hoisting mechanisms, vision systems, thermal monitoring and control systems, radiological monitoring systems, on-board safety systems, and auxiliary systems and instrumentation.

As indicated earlier, a preliminary design for the Emplacement Gantry mechanical system was presented in *Bottom/Side Lift Gantry Conceptual Design* (CRWMS M&O 2000c). The *Repository Rail Electrification Analysis* presented preliminary designs for providing power to the mobile emplacement vehicles (CRWMS M&O 1997c, section 7.2). It is planned that the Emplacement Gantry will share common on-board control and mobile communication technologies with other mobile-remote vehicles used within the potential repository. Initial designs and concepts for the Emplacement Gantry control and communication systems were discussed previously in Section 6.5. The remainder of this section addresses the other major systems of the Emplacement Gantry design.

Vehicle Locomotion and Braking—Reliable locomotion and braking systems are critical to the overall success of the Emplacement Gantry. All vehicle locomotion commands are issued and monitored by human operators who are remotely controlling the Emplacement Gantry. As shown in Figure 5, the Emplacement Gantry is designed with four independent direct current DC

drive motors, one located at each of the four wheel assemblies, also known as bogies or trucks. The four drive motors provide a level of redundancy, in that failure of individual drives would not jeopardize recovery of the gantry from the emplacement drift. The DC motors will interface directly to power and control circuitry housed in on-board electrical cabinets.

There are a wide variety of commercially available variable-speed drive motor control systems that could be adapted for use on the Emplacement Gantry. Electronic components that are sensitive to radiation effects will be mounted in high-density shielded electronic cabinets, while non-sensitive components can be mounted in non-shielded NEMA-rated enclosures.

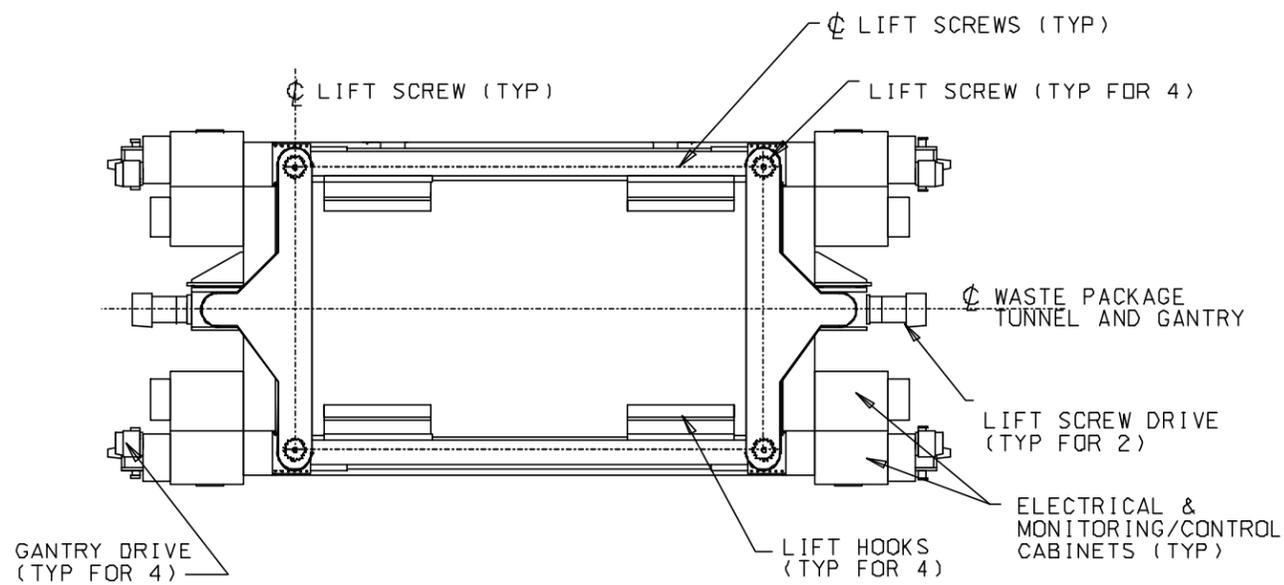
The motor control electronics will receive start/stop, position set-points, speed, and acceleration commands from its interface with the vehicle PLCs. The motor control electronics will perform all closed-loop position and speed control functions, and provide real-time position, speed, and acceleration feedback to the PLC. This drive concept has been successfully implemented by commercial crane companies in crane designs that have been approved by the NRC for handling nuclear materials.

There will be two independent fail-safe braking systems: a primary and a secondary (or emergency backup) system (CRWMS M&O 2000c, section 6.6.2). The braking system of the Emplacement Gantry will be designed such that in the event of power or communication loss, or vehicle control system malfunction, the braking system would engage and bring the vehicle to a stop. The braking systems will be designed with a series of parallel redundancies to eliminate the possibility of single-point failures.

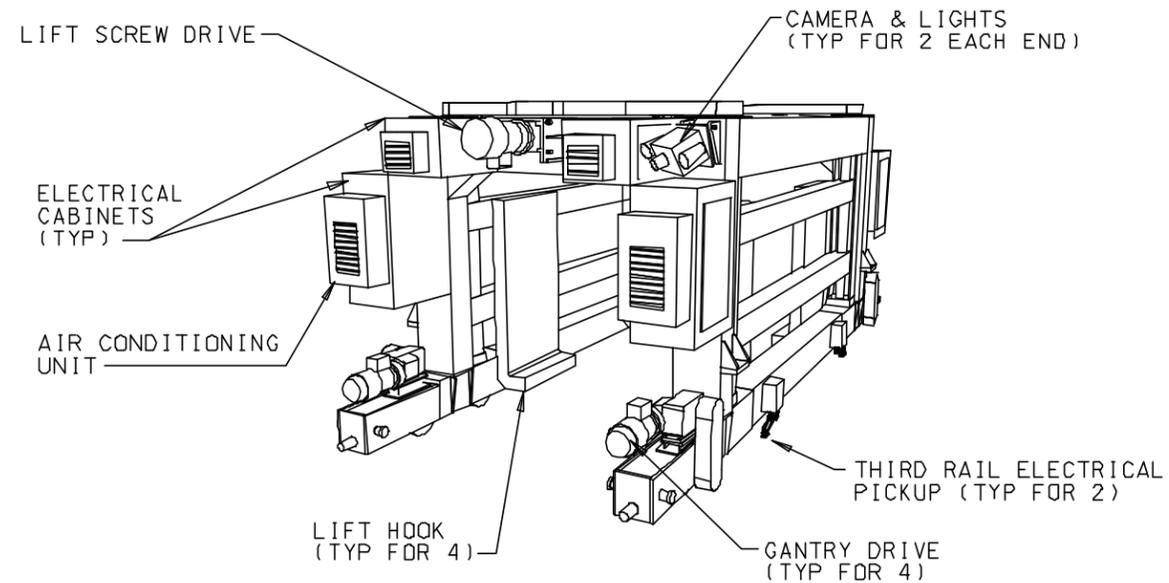
The drive motors for vehicle locomotion will be the primary consumers of power on-board the Emplacement Gantry. A preliminary analysis of the gantry electrification is provided in the *Repository Rail Electrification Analysis* (CRWMS M&O 1997c, section 7.2.5). Typically, drive motors become less efficient as ambient temperatures rise, although special high-temperature, radiation-hardened motors are available. Even though the Emplacement Gantry will operate in a relatively high-volume ventilated air stream, with moderate temperatures (27 °C), it may be necessary to provide an active cooling system for dissipating the heat generated by the motors. These cooling systems may be in the form of air conditioning units mounted to each of the electronics enclosures on the gantry.

There will be several safety features and design approaches included in the design that will essentially eliminate the possibility of derailment. These include: heavy-duty high-quality rails, high-quality rail mounts to the inverts, slow operating speeds, straight-line motion with no curves to negotiate, no rail switches inside emplacement drifts, double flanged wheels, fore- and aft-looking camera systems, and rail continuity sensing. (Note that excessive speed, loss of braking or control on hills, rounding curves too fast, and malfunctioning rail switches are typically the primary causes of derailment for rail-based vehicles. It is noted here that this design will not have to contend with these factors.)

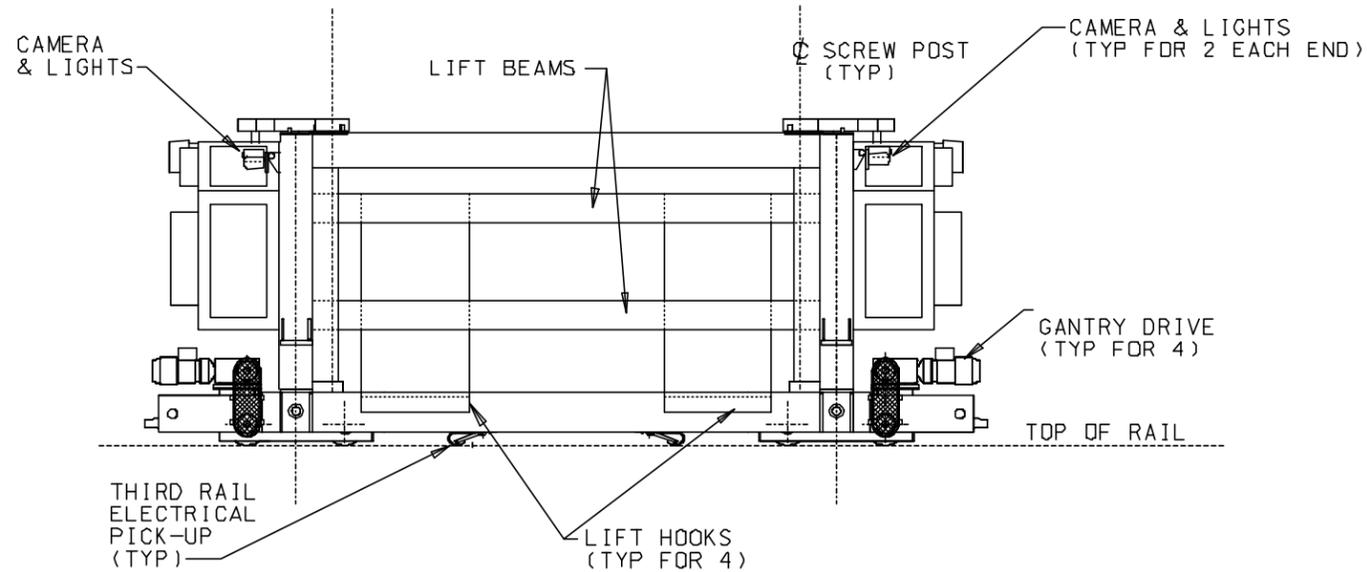
Waste Package Hoisting Mechanisms—The WP hoisting actuators are essential to the successful operation of the Emplacement Gantry. Initial mechanical designs for these actuator



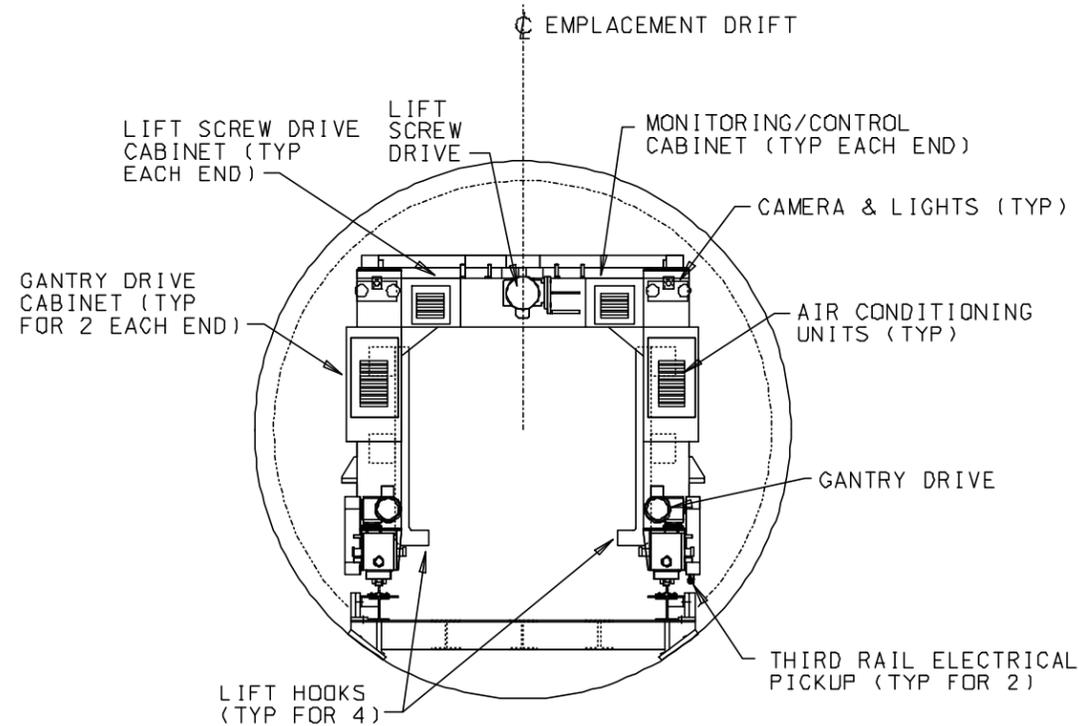
PLAN VIEW



PERSPECTIVE VIEW



ELEVATION VIEW



END VIEW

CAD FILE: ssm0226b.dgn

Figure 5. Emplacement Gantry

INTENTIONALLY LEFT BLANK

are presented in the *Bottom/Side Lift Gantry Conceptual Design* analysis (CRWMS M&O 2000c, section 6.4.1) and shown in Figure 5. It is evident by examination that these initial designs will require additional development and refinement in order to achieve the goal of eliminating areas of single-point failure within critical systems. With additional design work, it should be feasible to develop drive mechanisms that are fully redundant and fail-safe.

It is absolutely critical that the hoisting mechanisms perform their functions correctly and reliably. Recovery from stuck or otherwise malfunctioning mechanisms will be the subject of other design analyses, as will recovery from DBEs.

The design of the electronic drive controls for the lifting head and hoisting mechanism will employ several factors for safety and reliability. Triple and quad redundant drive components may be used. Backup controls and auxiliary power sources will be sufficient to safely lower and release a hoisted WP. The backup controls and power systems will be diverse, fully redundant, and physically separate from the primary actuation control systems.

Vision Systems—It is necessary that the human operators be provided with high-resolution real-time visual feedback of the remote operation of the Emplacement Gantry. High-resolution CCD (Charged Coupled Device) cameras are fairly inexpensive components. Their low cost and ease of integration can justify the use of multiple cameras. It is envisioned that several separate cameras can be used on the Emplacement Gantry. There can be two high-resolution, high-zoom, forward-looking cameras and two facing aft, each mounted to a motorized pan/tilt unit for positioning. There can also be two cameras mounted at the wheel level, called toe cameras, to provide imaging of the lower surfaces of the WPs and track surface. Special high-radiation tolerant cameras are available and can be used (CRWMS M&O 1995, page B-20; 1997b, pages 53 and 56). Coupled to the operation of the camera system is a series of external high-intensity lights. These light systems will consume considerable amounts of power, which, in turn, produces heat. The lights will be mounted on the external surfaces of the Emplacement Gantry and will be insulated to prevent radiating heat toward internal components.

Thermal Monitoring and Control Systems—Thermal control will be of key importance to the successful operation of the Emplacement Gantry. Strategies and design issues related to the thermal control of remotely operated vehicles were discussed in prior analyses (CRWMS M&O 1997b, section 7.5.2; 1996a; 1997e, section 7.6.6). They include: limiting time of exposure, thermal insulation (heat rejection) technologies and strategies, active and passive cooling systems for internally generated heat, use of thermally robust power and communication technologies, limiting (or alternating) the duty cycle of power-intensive components, use of low-power electronics and components, use of heat-tolerant electronics and hardware, and use of prudent thermal conduction paths for high-heat components.

There are two aspects to the thermal sensing instrumentation that will be used on the Emplacement Gantry. Some sensors will be used to monitor the performance of the gantry itself and the others will monitor the emplacement drift environment. Thermocouples and thermistors will be mounted throughout the Emplacement Gantry and on-board instrumentation to continuously monitor internal temperatures. Equipment operators will be alerted if any temperatures begin to approach predefined operational limits necessitating the removal of the

gantry from the emplacement drift. Air temperature can be measured continuously along the emplacement drift during an emplacement cycle.

Radiological Monitoring Systems—Various types of radiation monitoring sensors can be used in conjunction with the Emplacement Gantry. The radiation sensor package may consist of air radiation sensors that can continuously monitor the air for minute traces of radionuclide or tracer gases, indicating that a WP has developed a leak. Dosimeters can record cumulative dose radiation exposure to the Emplacement Gantry as a whole. Individual sensors may monitor dose exposures to sensitive electronics mounted inside the Emplacement Gantry electronic cabinets. These concepts are discussed in more detail in *Preliminary Analysis of Remote Monitoring & Robotic Concepts for Performance Confirmation* and *Remote Manipulation, Inspection and Sensing Technologies for Hazardous Environments* (CRWMS M&O 1997b, section 7.5.4; 1996d, SENSORS & INSTRUMENTATION section).

On-board Safety Systems—In the current design, the Emplacement Gantry is equipped with a fire detection and suppression system. The fire detection and suppression system is self-contained and will respond automatically in the event of a fire. The detection system will also be tied in to the vehicle's PLC system to provide operators with immediate notification in case of fire.

Auxiliary Systems and Instrumentation—As indicated earlier, the current design concept will utilize an electrified third-rail (conductor bar) system (CRWMS M&O 1997c, section 8.2). This concept is reliable, durable, thermally robust, and requires essentially no in-drift maintenance. Other design analyses will be performed regarding this subject to ensure that the power system rails or conductor bars will continue to perform under the expected repository conditions. As shown previously in Figure 5, redundant power pickup mechanisms will be employed to ensure a reliable and continuous source of power. In addition to this primary power system, there will also be an auxiliary backup power system that will provide a limited amount of emergency power. It should be sized to provide enough energy to operate a minimal set of control electronics, safely lower and release hoisted WPs, and possibly even drive the vehicle to the emplacement drift entrance. A storage battery source that is activated and operated only in an emergency may be sufficient. Other technologies are being investigated.

The Emplacement Gantry will be a flexible and versatile platform on which a variety of instruments can be mounted. Mechanical, electrical, and computing interfaces will be provided for quick installation and removal of modular instrument packages. The Emplacement Gantry can be designed to be easily reconfigured with new suites of instrumentation to accomplish a particular task. The control system will be designed such that, should one of these instruments fail, it would not adversely affect the otherwise normal and safe recovery of the vehicle from the emplacement drift. In addition to the thermal and radiological sensors, it may be useful to sample air gases and humidity levels across the drift. Air sampling systems could support the monitoring of other chemicals or gases of interest, such as carbon monoxide, or tracer gases if such are used in the WP.

6.6.2 Preliminary Emplacement Gantry Input/Output List

At this point in the design process, specific details of the Emplacement Gantry control system architecture, components, and interfaces have not yet been identified. However, it will be useful to develop a preliminary order-of-magnitude estimate of the quantity and type of I/O that may be needed. Section 6.4 of this analysis presents one of several feasible control architectures, with the gantry based on redundant PLCs. Table 5 is an initial estimate of the I/O interfaces that may be included in such a control system. Note that in the table below, AI = analog input, AO = analog output, DI = digital input, DO = digital output, SIO = serial I/O, and PIO = parallel I/O.

Table 5. Emplacement Gantry Control System Input/Output List

| Emplacement Gantry On-Board Systems | AI | AO | DI | DO | SIO | PIO |
|--|-----------|-----------|-----------|-----------|------------|------------|
| I. Gantry Power System | | | | | | |
| Power Pickup Status Monitoring (Voltage, Power) | 4 | | 4 | 2 | | |
| Power Distribution System (Voltage & Current Levels) | 8 | | 2 | 2 | | |
| | | | | | | |
| II. Gantry Communication System | | | | | | |
| Communication System Status | | | 4 | 4 | | |
| Communication System Interfaces | | | | | 2 | 2 |
| | | | | | | |
| III. Gantry Locomotion System | | | | | | |
| Drive Motor Control Unit | | | | | 2 | 2 |
| Drive Motor Control: Power On/Off | | | | 2 | | |
| Drive Motor Control: Status | | | 2 | | | |
| Drive Motor Control : Direction | | | | 2 | | |
| Drive Motor Control: Fine Positioning | | | | 2 | | |
| Drive Motor Control: Speed | | | | 2 | | |
| Drive Motor Control: Acceleration | | | | 2 | | |
| Gantry Coarse Positioning System | | | 2 | 2 | | 2 |
| Power, Voltage, Current | 12 | | | | | |
| Primary Brake Engage | | | | 2 | | |
| Primary Brake Status | | | 2 | | | |
| Secondary Brake Engage | | | | 2 | | |
| Secondary Brake Status | | | 2 | | | |
| Temperature | 8 | | | | | |
| | | | | | | |
| IV. Actuation Systems: Lifting Head & Hoist | | | | | | |
| Actuator Motor Control Unit | | | | | 2 | 2 |
| Actuator Motor Control: Power On/Off | | | | 2 | | |
| Actuator Motor Control: Status | | | 2 | | | |
| Actuator Motor Control : Direction | | | | 2 | | |
| Actuator Motor Control: Position | | | | 2 | | |
| Actuator Motor Control: Speed | | | | 2 | | |
| Limit Switches | | | | 16 | | |

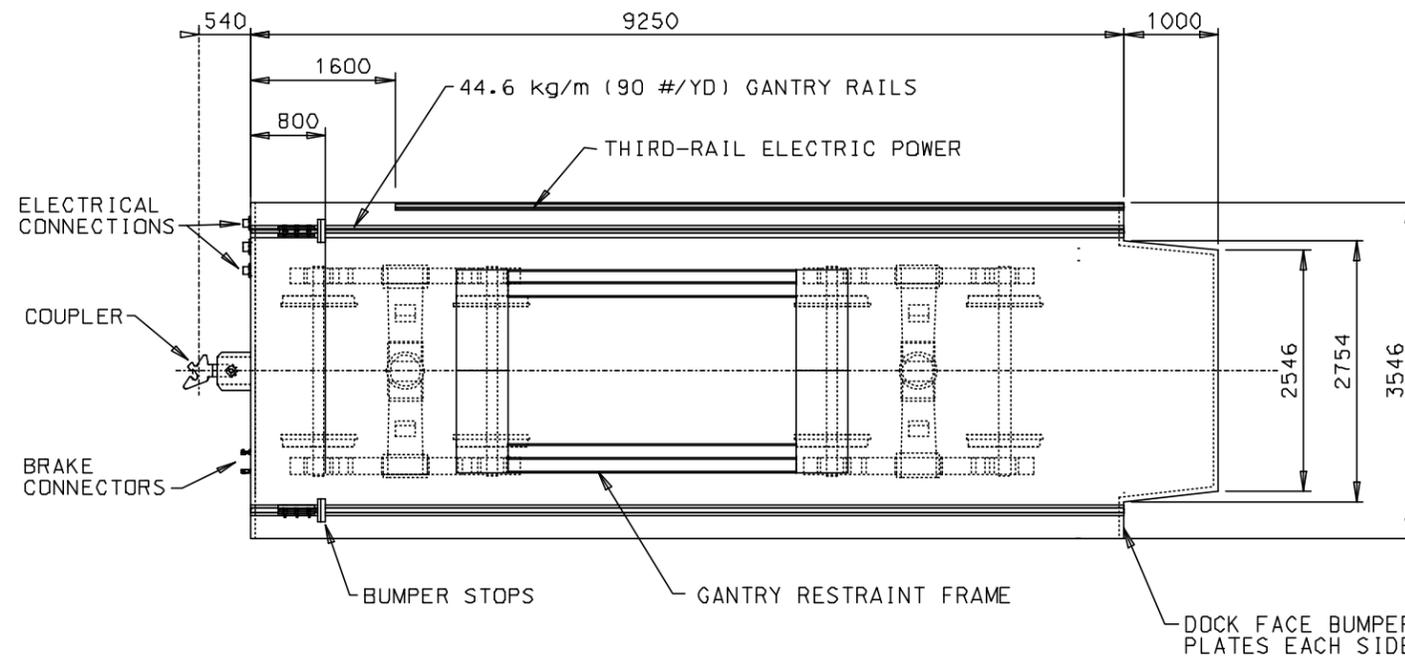
| Emplacement Gantry On-Board Systems | AI | AO | DI | DO | SIO | PIO |
|---|-----------|-----------|-----------|-----------|------------|------------|
| Load Sensors | 8 | | | | | |
| Power, Voltage, Current | 12 | | | | | |
| Temperature | 8 | | | | | |
| V. Gantry Vision System | | | | | | |
| Video Switch Controller (8 Cameras) | | | 8 | | | 2 |
| Video Controls (Power, Zoom, Balance) | | | 4 | 4 | | |
| Pan/Tilt Unit Controller (4 units) | | 4 | 4 | 2 | | 2 |
| Lighting System | | 4 | 4 | | | |
| VI. Gantry Thermal Monitoring & Control System | | | | | | |
| Electronic Enclosure Thermal Monitoring | 8 | | | | | |
| Electronic Enclosure Cooling | | | 2 | | 2 | |
| Motor Housings Thermal Monitoring | 4 | | | | | |
| Motor Housing Cooling | | | 2 | | 2 | |
| Environmental Temperature Monitoring | 4 | | | | | |
| VII. Radiological Monitoring System | | | | | | |
| Equipment Exposure Dosimetry | 4 | | | 4 | | |
| Environmental Monitoring | 4 | | | 4 | | |
| VIII. Safety & Auxiliary Systems | | | | | | |
| Backup Power System | 2 | | 2 | 2 | | |
| Fire Suppression System | | | 2 | 2 | | |
| Preliminary Estimate of Emplacement Gantry Control System I/O Totals: | | | | | | |
| | 86 | 8 | 48 | 66 | 10 | 12 |

The preliminary estimate of control system I/O totals for the Emplacement Gantry reveal that the vehicle will be a moderately complex system. Significant design work will be required to determine the exact I/O requirements. Focused analyses on each of the eight gantry systems identified in the I/O list are recommended.

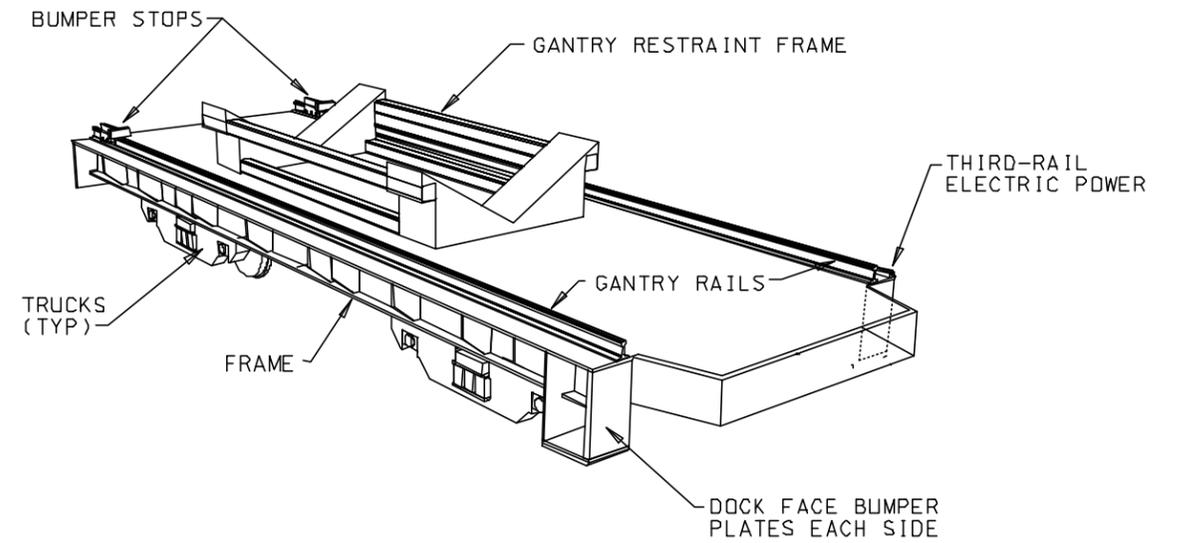
6.6.3 Emplacement Gantry Carrier

The Emplacement Gantry Carrier is basically a rail-car device that will be used to shuttle the Emplacement Gantry between emplacement drifts and transport the Emplacement Gantry to the surface storage and maintenance facility (see Figure 6). The Emplacement Gantry Carrier will be moved by the Transport Locomotives (see section 6.7).

The Emplacement Gantry Carrier will have relatively few, but nonetheless important, systems to be controlled. It will not be equipped with its own electronic control system. Rather, all control and monitoring functions will interface directly with the Transport Locomotive I/O system.

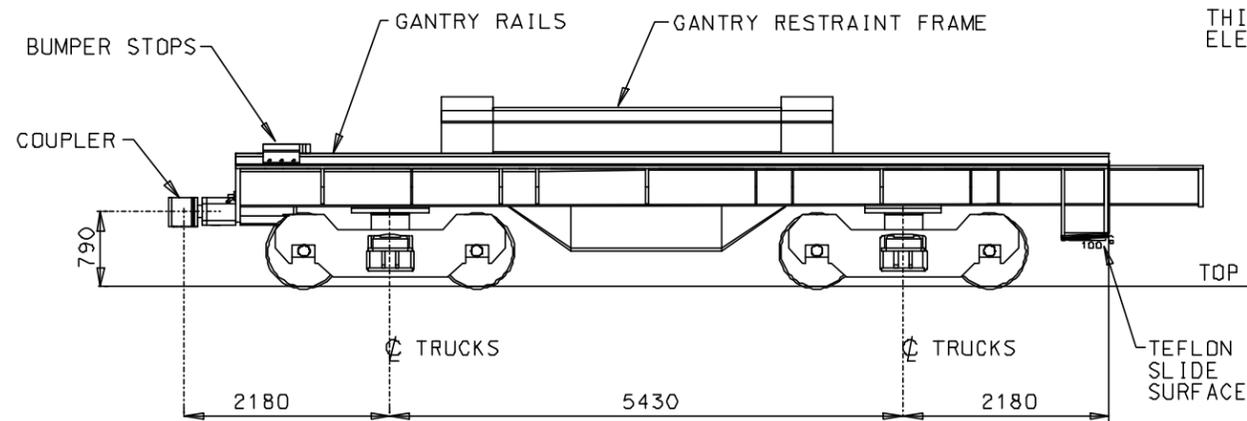


PLAN

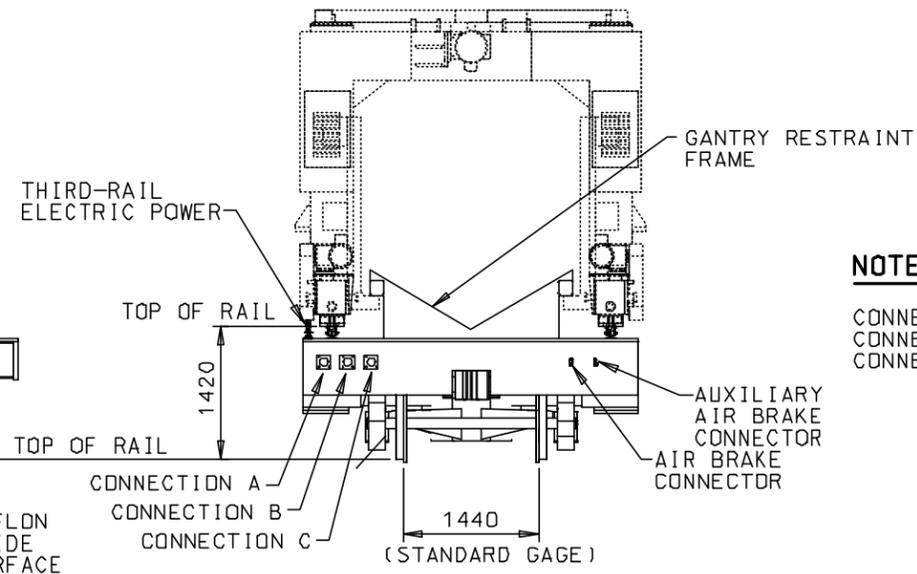


PERSPECTIVE VIEW

CAD FILE: megan99carrier.dgn



ELEVATION



END VIEW

NOTES:

- CONNECTION A - 650 V DC TROLLEY POWER
- CONNECTION B - CONTROL POWER
- CONNECTION C - CONTROL SIGNALS

ALL DIMENSIONS ARE SHOWN IN MILLIMETERS UNLESS OTHERWISE NOTED

Figure 6. Emplacement Gantry Carrier

INTENTIONALLY LEFT BLANK

The Carrier will be equipped with quick-disconnect feed-through connectors to provide pneumatic, electrical power, and analog and digital control interfaces between the Transport Locomotive and the Carrier.

The Carrier will have its own independent fail-safe braking system that will be energized via the pneumatic connection to the locomotive. The Carrier will also be equipped with a gantry restraint frame, as seen in Figure 6, that may include electrical contact switch feedback for safety interlocks. A third-rail (conductor bar) on the top deck of the Carrier will provide electric power to the Emplacement Gantry so that it can be driven on and off the Carrier.

6.6.4 Emplacement Gantry Carrier Control Interfaces

A preliminary estimate of the Emplacement Gantry Carrier control system I/O is provided in Table 6 below. Note that in the table below, AI = analog input, AO = analog output, DI = digital input, DO = digital output, SIO = serial I/O, and PIO = parallel I/O.

Table 6. Emplacement Gantry Carrier Control System Input/Output List

| Emplacement Gantry Carrier Control System I/O | AI | AO | DI | DO | SIO | PIO |
|---|-----------|-----------|-----------|-----------|------------|------------|
| I. Carrier Braking System | | | | | | |
| Primary Brake Engage | | | | 2 | | |
| Primary Brake Status | | | 2 | | | |
| Secondary Brake Engage | | | | 2 | | |
| Secondary Brake Status | | | 2 | | | |
| Temperature | 8 | | | | | |
| | | | | | | |
| II. Gantry Power System | | | | | | |
| Conductor Bar Power: On/Off | | | 2 | 2 | | |
| Conductor Bar Power Level | 2 | | 2 | 2 | | |
| | | | | | | |
| III. Transport Locomotive Interface | | | | | 1 | 1 |
| | | | | | | |
| IV. Emplacement Gantry Interface | | | | | 1 | 1 |
| | | | | | | |
| Preliminary Estimate of Emplacement Gantry Carrier Control System I/O Totals: | 10 | | 8 | 8 | 2 | 2 |

6.7 TRANSPORT LOCOMOTIVE

The Transport Locomotives will serve as the multi-purpose prime movers of equipment and personnel and will be used in almost every aspect of subsurface operations. They will be used not only for emplacement activities, but also for retrieval, performance confirmation, drip shield installation and caretaker activities. During emplacement operations, the Transport Locomotives will be used in tandem to haul WPs in the Waste Package Transporter from the Waste Handling Building to the entrance of the emplacement drifts. The Transport Locomotives will also be used to shuttle the Emplacement Gantry from drift to drift and periodically return it to the servicing

area for maintenance. The Transport Locomotives may also be used to move personnel or materials as needed within the subsurface operations area.

According to *Mobile Waste Handling Support Equipment* (CRWMS M&O 1998c, section 7.3.1), current concepts for the Transport Locomotives are based on commercially available 50-ton mining locomotives. Power for the locomotives will be provided by an overhead trolley system, and the locomotives will be designed for both direct manual control and wireless remote control (CRWMS M&O 1997c, section 8.2). The locomotives will be remotely operated when conditions are unsafe for human operators, such as, all operations near the emplacement drift docking areas.

Due to the vital importance and anticipated high use of the Transport Locomotives, the fundamental design goals are to develop a fleet of highly reliable, durable, and robust locomotives that can safely perform their intended functions over the entire range of possible operating conditions. As discussed in previous sections, the design approach will be to identify critical systems within the locomotives and seek to eliminate single-point failure areas by using redundant high-quality components and backup systems.

The current design layout of the Transport Locomotive is shown in Figure 7. The purpose of the following sections is to describe the basic control elements of the Transport Locomotives.

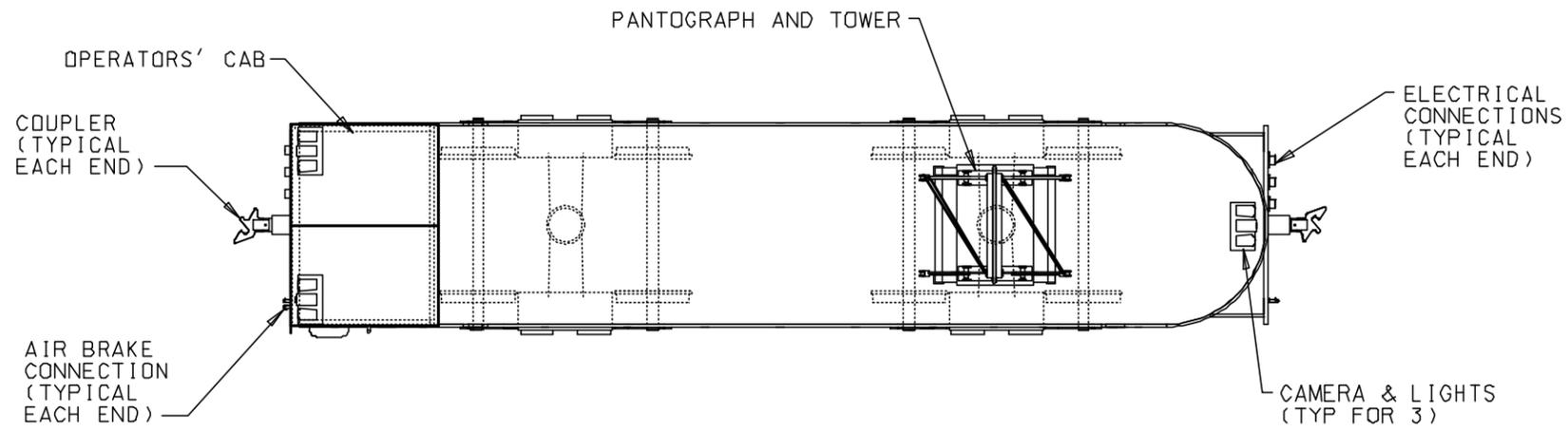
6.7.1 Transport Locomotive Control Functions

The design of the Transport Locomotive will be composed of several key systems, including: mechanical structure, on-board control system, power supply and distribution systems, communication systems, locomotion and braking systems, environmental and performance monitoring systems, operator interfaces, lighting and camera systems, on-board safety systems, and auxiliary systems.

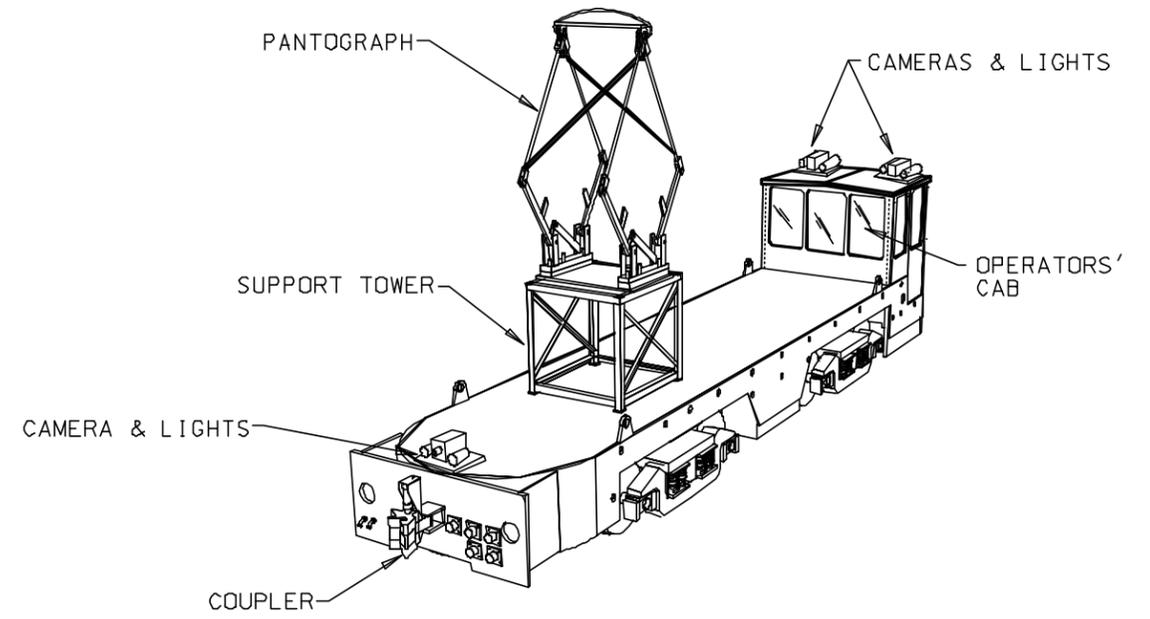
Some of these systems are addressed in other, recently completed analyses. Preliminary designs of the mechanical structure of the Transport Locomotives are presented in *Mobile Waste Handling Support Equipment* (CRWMS M&O 1998c, section 7.3), and designs for the overhead trolley power system are presented in *Repository Rail Electrification Analysis* (CRWMS M&O 1997c, section 7.4).

A general architecture for the on-board vehicle control and communication systems is presented in Section 6.5 of this analysis. In addition to controlling the operation of the locomotive, the control system for the Transport Locomotives will have several unique interfaces. One key interface will be between the two Transport Locomotives when used in tandem to transport a full Waste Package Transporter from the surface Waste Handling Building down into the emplacement drift area. Tandem control permits one operator to operate two locomotives as a single unit. These interfaces are discussed further in the next section (Section 6.7.2).

The Transport Locomotives will also interface with, and control, various functions on the Waste Package Transporter and the Emplacement Gantry Carrier. The interfaces between the Transport Locomotive and the Emplacement Gantry Carrier are briefly discussed in Section 6.6.4, while

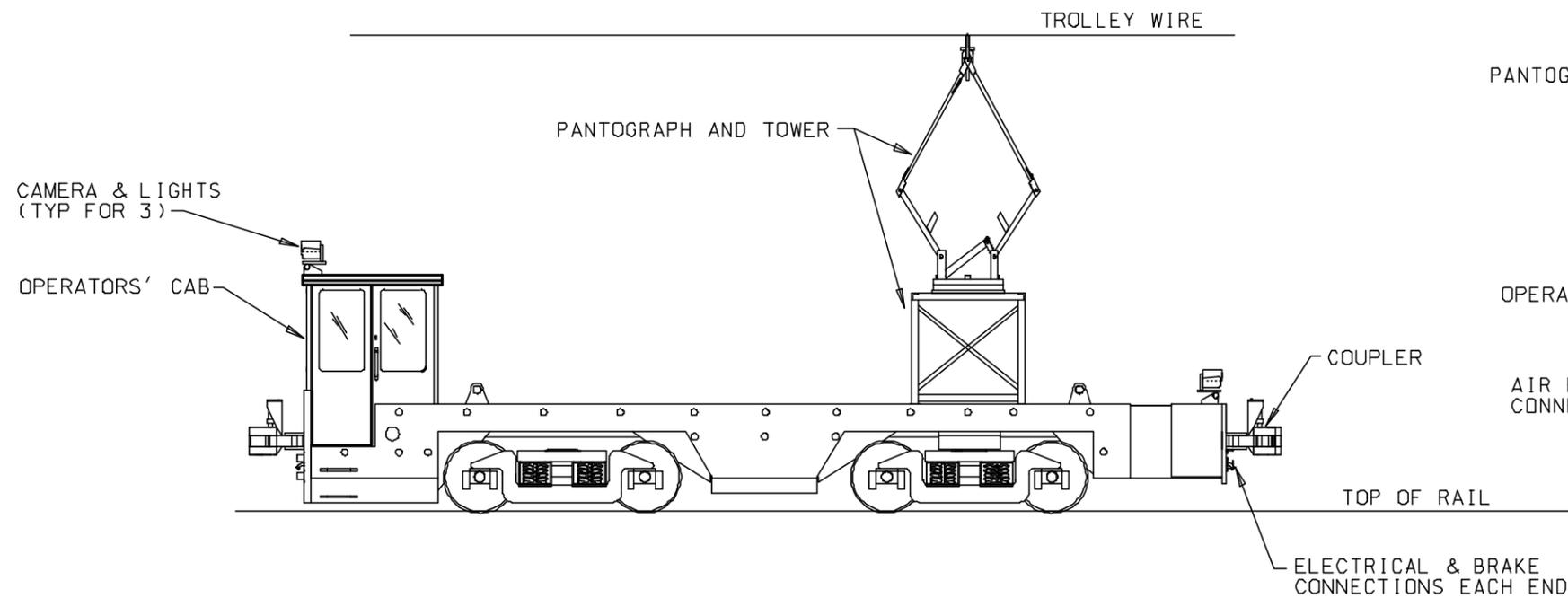


PLAN VIEW

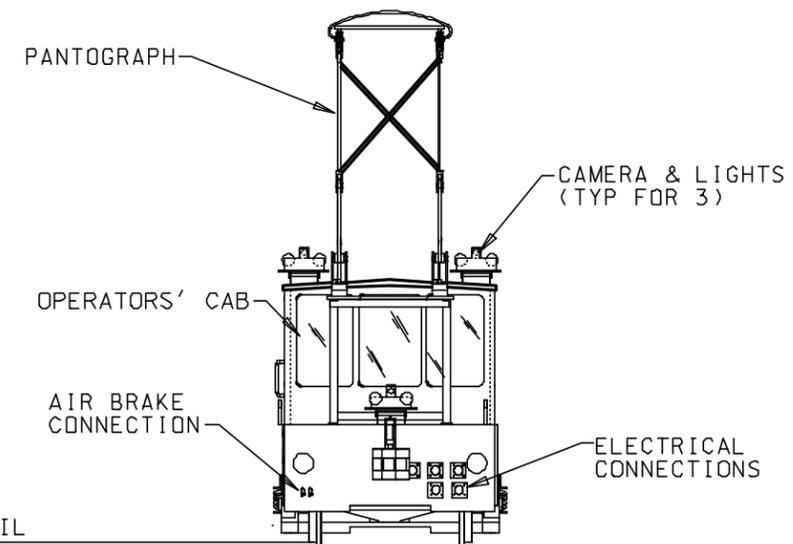


PERSPECTIVE VIEW

CAD FILE: me0223a.dgn



ELEVATION VIEW



END VIEW

Figure 7. Transport Locomotive

INTENTIONALLY LEFT BLANK

the interfaces between the locomotives and the Waste Package Transporter are discussed in Section 6.7.2.

Locomotion & Braking Systems—The size, type, capacity, and configuration of the locomotion and braking systems on the Transport Locomotives will be very different than those discussed previously for the Emplacement Gantry. Nevertheless, the basic control system will be quite similar.

The main tractive force for the locomotive drive will be provided by multiple DC series-wound motors. Many locomotives used in subsurface applications utilize series-wound motors that are mounted in a trans-axle configuration with a single reduction-spur gear transmission. In a series-wound motor, the field windings are connected in series to the armature and, therefore, all of the current flows through both the field and armature.

The motor output torque is directly proportional to the motor input current and the magnetic flux of the motor. Any increase in current also increases the flux. Since both the current and the flux increase at the same rate, the motor output torque varies as the square of the current. Series-wound motors also have excellent starting torque characteristics. Furthermore, according to Hustrulid (1982, page 1230) DC series-wound motors have an outstanding record in terms of reliability, simplicity, and ease of maintenance.

Controlling the DC series-wound motors is a matter of regulating input current and the applied voltage. Many locomotives in use today employ silicon-controlled rectifier (SCR) technology to control motor voltage and speed. This is a common, well proven control technology that is readily applicable to either manual or remote-control interfaces. Another important function of the motor-control circuitry is to limit inrush starting current that may otherwise damage the motor. As indicated in previous technology surveys, there is a wide variety of commercial motor controllers available (CRWMS M&O 1995, Appendix B; 1996c).

The current design concept calls for the Transport Locomotives to be equipped with a highly reliable airbrake system typical of those found in mining and rail transportation industries (Air Brake Association 1975, chapter VI; Air Brake Association 1998, chapter II; Hustrulid 1982, pages 1233,1234). Control of the airbrake system is typically a matter of setting and releasing a series of solenoid valves. For the critical application within the repository, the brake design will utilize two independent braking systems. The control and monitoring of the primary braking system will be performed by the locomotive's on-board PLC. Secondary fail-safe braking systems can be implemented using an automatic spring-loaded mechanism which will be monitored by the on-board PLC, but whose actuation is independent from the electronic control system. Dynamic braking techniques are implemented on many conventional locomotives to convert the mechanical energy of a moving train into electrical energy, that can be either dissipated as heat in a resistor bank or used to back-feed the power supply system, which is known as regenerative braking. This technique is not used to bring the train to a full stop, however. Further investigation is needed to determine if this technique would be practical and efficient for locomotives used within the potential repository. Typically, regenerative braking is not used in mining applications where down-slope grades are relatively short.

Environmental and Performance Monitoring Systems—The Transport Locomotives will be designed with an extensive thermal monitoring and control system similar to that described in Section 6.5. The locomotives will be heavily instrumented to monitor a variety of internal and external parameters important to safe vehicle control and operation. These include: monitoring temperatures of key systems throughout the locomotive, monitoring external temperatures and radiation levels, monitoring current draw and voltage levels, etc. This information will be fed back to the on-board controller and relayed to operators located at the remote control console.

Operator Interfaces—The Transport Locomotives will be equipped with both manual and remote control interfaces. The operator's cab on-board will be outfitted with conventional locomotive manual controls, including throttle and brake controls, as well as performance gages and indicators. During manual operation, the locomotives will be continuously monitored for safe and proper operation by supervisory operators in the remote command center. There will be a switch for configuring the locomotive to operate as either the primary or secondary locomotive when used in tandem mode. There will also be a switch for configuring the locomotive for either remote or manual control. When in remote control mode, locomotive functions will be initiated and monitored by personnel at a remote control console. These remote operators will be provided with extensive audio and visual feedback of the locomotives performance. As indicated in the *Subsurface Repository Remote Handling & Robotics Evaluation Report* and the *Review of Safety-Related Data Communication Systems* (CRWMS M&O 1995, section 5.1.2; 1998a, section 7.3.1), safe and reliable remote control technologies for locomotives have been developed over the last 20 years.

The Transport Locomotive lighting and camera systems, on-board safety systems, and auxiliary systems will be similar to those described in Section 6.5 for the Emplacement Gantry.

6.7.2 Interfaces between Primary and Secondary Transport Locomotives

Two Transport Locomotives working in tandem will be used to haul a loaded Waste Package Transporter from the Waste Handling Building to the emplacement drift area within the potential repository. The Transporter will be positioned between the two locomotives. The operation of these two locomotives will be closely coupled to work in unison to accomplish this task. The locomotives will be virtually identical. By configuring the appropriate switch settings, one locomotive will be selected as the lead or primary locomotive, and the other will be designated as the secondary. The hardware and software required to operate in either the primary or secondary role will reside on each locomotive.

In tandem control, one operator will be able to control both locomotives. The operator, who will ride on-board the primary locomotive, will issue speed, acceleration, and braking commands to the primary locomotive. These commands will be translated into corresponding commands that will drive the secondary locomotive in a compliant manner. It is important that the secondary locomotive act in concert with, and not against, the primary locomotive. One way that this can be accomplished is by closed-loop control of the draw-bar towing and pushing forces. The control system on-board the secondary locomotive will have the capacity to monitor the performance of the primary locomotive, and, in the event of a malfunction, lead control can be temporarily switched over to the secondary locomotive (see Figure 8).

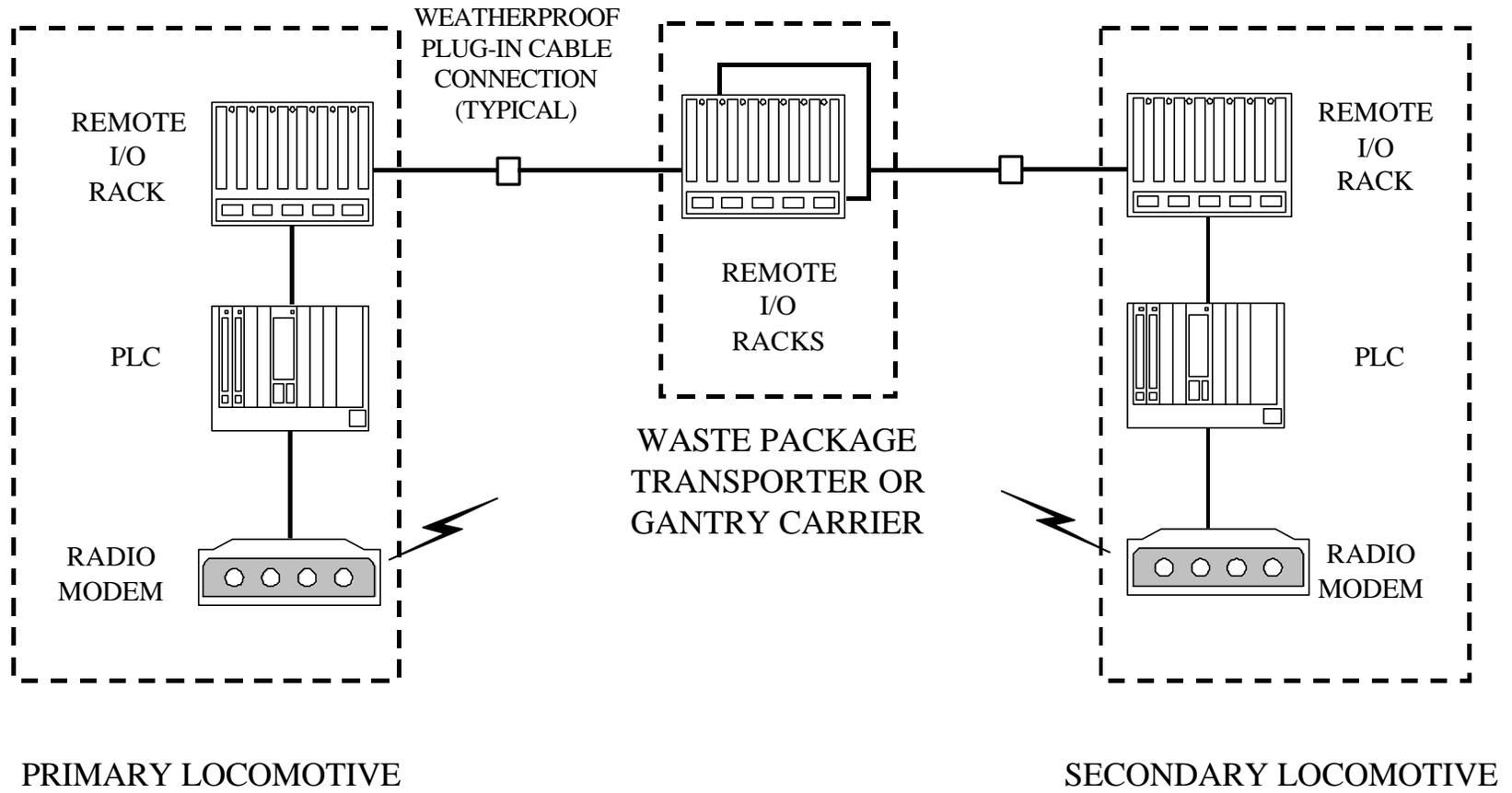


Figure 8. Control Interfaces for Locomotives in Tandem Control Configuration

There will be electrical and pneumatic interfaces between the primary and secondary locomotives. These interfaces will be facilitated by quick-disconnect connections located at the front and rear of each locomotive. When the locomotives are in the tandem-control configuration, the electrical and pneumatic connections will be provided by feed-through connections on the Waste Package Transporter.

6.7.3 Transport Locomotive Input/Output List

At this point in the design process, specific details of the Transport Locomotive control system architecture, components, and interfaces have not been identified. However, it is useful to develop a preliminary order-of-magnitude estimate of the quantity and type of I/O that may be needed. Section 6.5 of this analysis presents one of several feasible control architectures, and is based on redundant PLCs. Table 7 is an initial estimate of the I/O interfaces that may be included in such a control system. Note that in the table below, AI = analog input, AO = analog output, DI = digital input, DO = digital output, SIO = serial I/O, and PIO = parallel I/O.

Table 7. Transport Locomotive Control System Input/Output List

| Transport Locomotive On-Board Systems | AI | AO | DI | DO | SIO | PIO |
|--|-----------|-----------|-----------|-----------|------------|------------|
| I. Transport Locomotive Power System | | | | | | |
| Power Pickup Status Monitoring (Voltage, Power) | 4 | | 4 | 2 | | |
| Power Distribution System (Voltage & Current Levels) | 8 | | 2 | 2 | | |
| II. Transport Locomotive Communication System | | | | | | |
| Communication System Status | | | 4 | 4 | | |
| Communication System Interfaces | | | | | 2 | 2 |
| III. Locomotion System | | | | | | |
| Drive Motor Control Unit (one fore and one aft) | | | | | 2 | 2 |
| Drive Motor Control: Power On/Off | | | | 2 | | |
| Drive Motor Control: Status | | | 2 | | | |
| Drive Motor Control : Direction | | | | 2 | | |
| Drive Motor Control: Fine Positioning | | | | 2 | | |
| Drive Motor Control: Speed | | | | 2 | | |
| Drive Motor Control: Acceleration | | | | 2 | | |
| Locomotive Coarse Positioning System | | | 2 | 2 | | 2 |
| Power, Voltage, Current | 12 | | | | | |
| Primary Brake Engage | | | | 2 | | |
| Primary Brake Status | | | 2 | | | |
| Secondary Brake Engage | | | | 2 | | |
| Secondary Brake Status | | | 2 | | | |
| Brake Temperature Sensors | 8 | | | | | |
| IV. Tandem Locomotive Control Interface | | | | | | 1 |

| Transport Locomotive On-Board Systems | AI | AO | DI | DO | SIO | PIO |
|---|-----------|-----------|-----------|-----------|------------|------------|
| V. Locomotive Interface with Waste Package Transporter | | | | | | 1 |
| VI. Locomotive Interface with Gantry Carrier | | | | | | 1 |
| VII. Vision System | | | | | | |
| Video Switch Controller (4 Cameras) | | | 4 | | | 2 |
| Video Controls (Power, Zoom, Balance) | | | 4 | 4 | | |
| Pan/Tilt Unit Controller (2 units) | | 4 | 4 | 2 | | 1 |
| Lighting System | | 4 | 4 | | | |
| VIII. Thermal Monitoring & Control System | | | | | | |
| Electronic Enclosure Thermal Monitoring | 8 | | | | | |
| Electronic Enclosure Cooling | | | 2 | | 2 | |
| Motor Housings Thermal Monitoring | 4 | | | | | |
| Motor Housing Cooling | | | 2 | | 2 | |
| Environmental Temperature Monitoring | 4 | | | | | |
| IX. Radiological Monitoring System | | | | | | |
| Equipment Exposure Dosimetry | 4 | | | 4 | | |
| Environmental Monitoring | 4 | | | 4 | | |
| X. Safety & Auxiliary Systems | | | | | | |
| Backup Power System | 2 | | 2 | 2 | | |
| Fire Suppression System | | | 2 | 2 | | |
| Preliminary Estimate of Transport Locomotive Control System I/O Totals: | 56 | 8 | 42 | 42 | 4 | 12 |

The preliminary estimate of control system I/O totals for the Transport Locomotive indicates that the vehicle will be a moderately complex system. Significantly more design work will be required to determine more exact I/O requirements. Focused analyses on several of the sub-systems identified in the I/O list are recommended.

6.8 WASTE PACKAGE TRANSPORTER

The Waste Package Transporter is a massive rail car that will be used to transport the WPs in a completely enclosed and highly shielded enclosure from the Waste Handling Building at the surface, down into the emplacement drift area of the potential repository. The Waste Package Transporter is highly shielded in order to protect personnel that may need to work in the vicinity through which the Transporter will travel. A preliminary mechanical design for the Waste Package Transporter was recently the subject of a separate analysis (CRWMS M&O 2000b, section 6); the basic mechanical layout can be seen in Figure 9. In its current design configuration, the shielding used to form the walls, floor, crown and doors of the Waste Package

Transporter will be over 260-mm thick. The shielding material will be multiple layers of stainless and carbon steels, and a borated polyethylene material.

The Waste Package Transporter will be equipped with its own set of air brakes and a redundant backup set of spring-loaded fail-safe brakes. The Waste Package Transporter will have a set of double doors at one end which will be opened and closed by two heavy-duty gear motors mounted in-line with the axis of the door hinges.

Inside the Waste Package Transporter will be a WP loading and unloading mechanism. The loading mechanism will consist of two main systems: a rail-based shuttle mechanism, and a rigid-chain drive system, which will be used for extending and retracting the shuttle car during loading and unloading activities. Both of these component systems will have multiple positioning sensors and other types of performance feedback sensors. Also inside the Waste Package Transporter will be a camera system for remote viewing, along with radiation and thermal monitoring instrumentation.

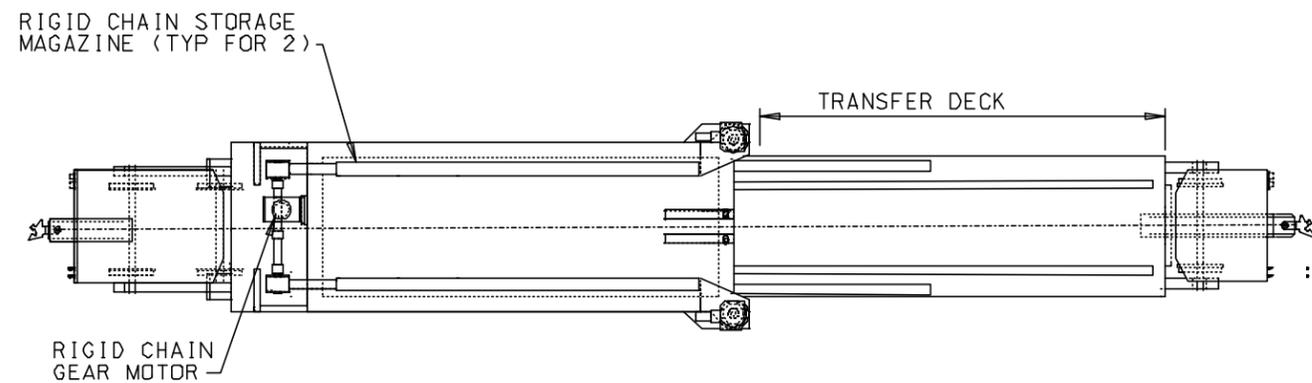
The operation and functions of the Waste Package Transporter will be remotely controlled. Control commands will originate either from the operator located on the primary locomotive, or from operators located at the remote control console. In either case, the control signals will be processed by the PLC-based control system located on the primary Transport Locomotive, and then communicated to a PLC-based control system located on the Waste Package Transporter. The PLC on the primary locomotive will monitor and check all operations and system performance parameters of the Waste Package Transporter.

The overall reliability of Waste Package Transporter systems, particularly the loading mechanisms, will need to be very high. The initial mechanical designs will continue to undergo further development and refinement in order to achieve the goal of implementing fully redundant and fail-safe devices within critical systems and eliminating areas of potential single-point failure. The difficulties resulting from a stuck or otherwise malfunctioning loading mechanism warrant extensive efforts to design these systems to be exceptionally reliable.

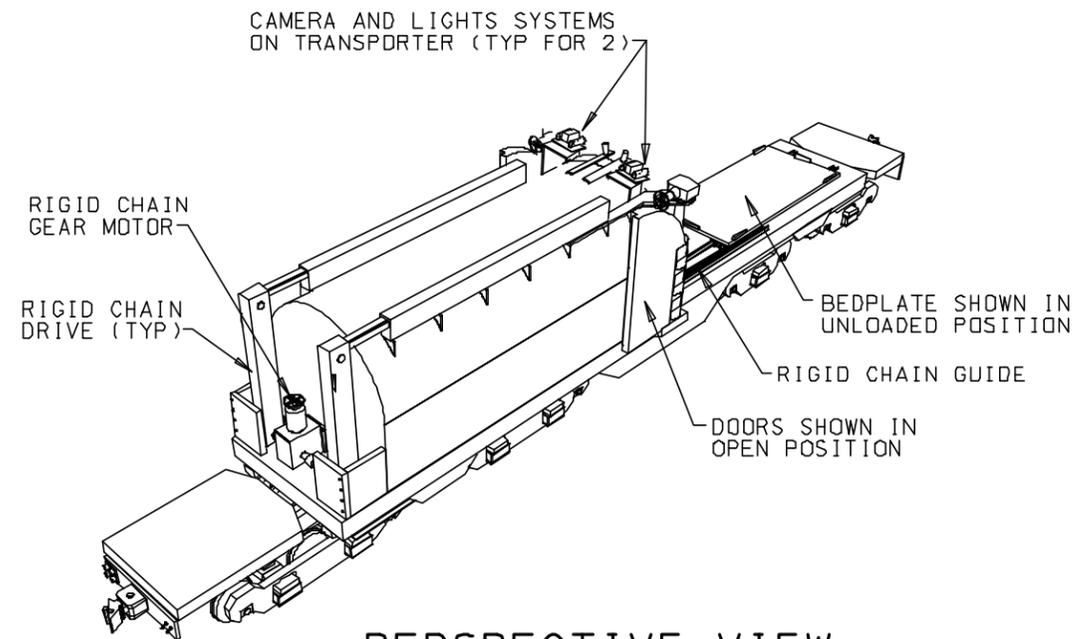
When empty, the Waste Package Transporter will be fully accessible inside and out by personnel for routine and preventative maintenance. Because the Waste Package Transporter PLC control system will be mounted outside the protective shielding, it will be directly accessible by personnel and, therefore, may not require the added complexity of being fully redundant.

6.8.1 Preliminary Waste Package Transporter Input/Output List

The Waste Package Transporter will utilize an on-board PLC for managing and controlling all on-board control functions. The PLC will interface directly with the control system of the Transport Locomotives. At this point in the design process, specific details of the Waste Package Transporter control system architecture, components, and interfaces have not been identified. However, it will be useful to develop a preliminary order-of-magnitude estimate of the quantity and type of I/O that may be needed. Table 8 is an initial estimate of the I/O interfaces that may be included in such a control system. Note that in the table below, AI = analog input, AO = analog output, DI = digital input, DO = digital output, SIO = serial I/O, and PIO = parallel I/O.

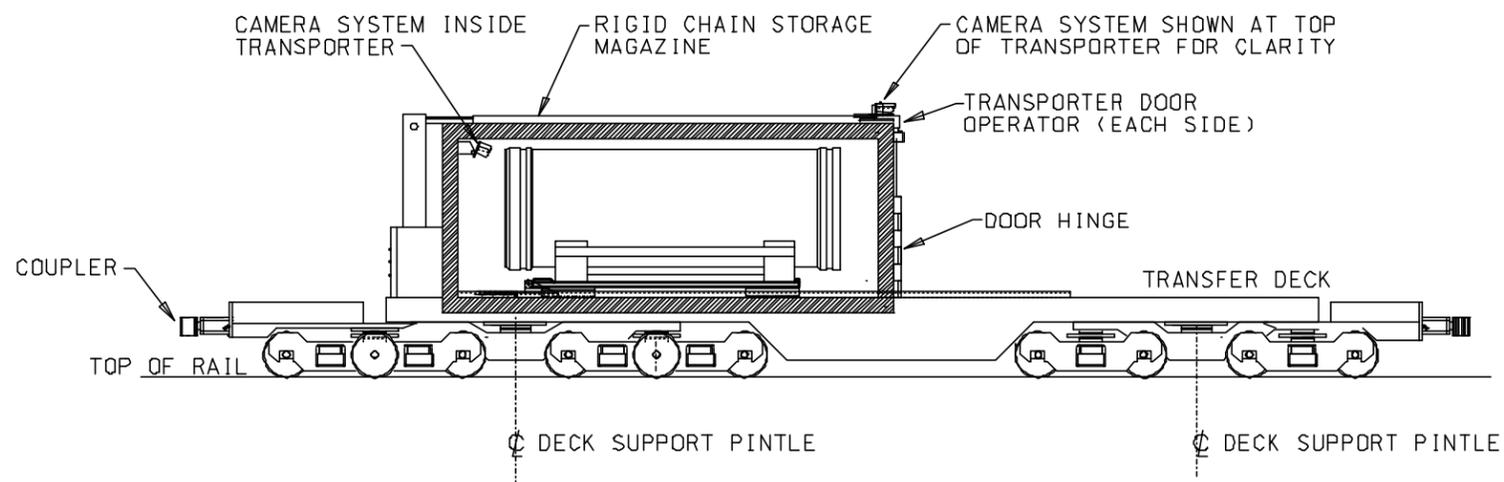


PLAN VIEW

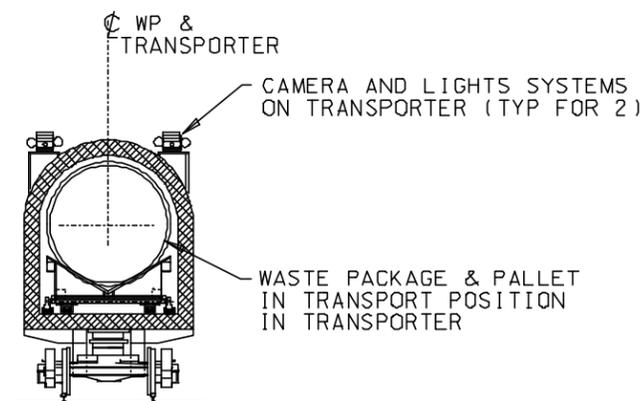


PERSPECTIVE VIEW

CAD FILE: me0224a.dgn



ELEVATION VIEW



CROSS SECTION

Figure 9. Waste Package Transporter

INTENTIONALLY LEFT BLANK

Table 8. Waste Package Transporter Control System Input/Output List

| Waste Package Transporter On-Board Systems | AI | AO | DI | DO | SIO | PIO |
|---|-----------|-----------|-----------|-----------|------------|------------|
| I. Waste Package Transporter Braking System | | | | | | |
| Primary Brake Engage | | | | 2 | | |
| Primary Brake Status | | | 2 | | | |
| Secondary Brake Engage | | | | 2 | | |
| Secondary Brake Status | | | 2 | | | |
| Brake Temperature Sensors | 8 | | | | | |
| | | | | | | |
| II. Actuation Systems: Loading Mechanism | | | | | | |
| Actuator Motor Control Unit | | | | | 2 | 2 |
| Actuator Motor Control: Power On/Off | | | | 2 | | |
| Actuator Motor Control: Status | | | 2 | | | |
| Actuator Motor Control : Direction | | | | 2 | | |
| Actuator Motor Control: Position | | | | 2 | | |
| Actuator Motor Control: Speed | | | | 2 | | |
| Limit Switches | | | | 8 | | |
| Power, Voltage, Current | 6 | | | | | |
| Motor Temperature Sensors | 8 | | | | | |
| | | | | | | |
| III. Transporter Vision System | | | | | | |
| Video Switch Controller (2 Cameras) | | | 2 | | | 1 |
| Video Controls (Power, Zoom, Balance) | | | 2 | 2 | | |
| Pan/Tilt Unit Controller (1 units) | | 2 | 2 | 1 | | 1 |
| Lighting System | | 2 | 2 | | | |
| | | | | | | |
| IV. Waste Package Transporter Thermal Monitoring & Control System | | | | | | |
| Electronic Enclosure Thermal Monitoring | 8 | | | | | |
| Electronic Enclosure Cooling | | | 2 | | 2 | |
| Motor Housings Thermal Monitoring | 4 | | | | | |
| Motor Housing Cooling | | | 2 | | 2 | |
| Environmental Temperature Monitoring | 4 | | | | | |
| | | | | | | |
| V. Radiological Monitoring System | | | | | | |
| Equipment Exposure Dosimetry | 4 | | | 4 | | |
| Environmental Monitoring | 4 | | | 4 | | |
| | | | | | | |
| VI. Locomotive Interface with Waste Package Transporter | | | | | | 1 |
| | | | | | | |
| Preliminary Estimate of Waste Package Transporter Control System I/O Totals: | 46 | 4 | 18 | 31 | 6 | 5 |

The preliminary estimate of control system I/O totals for the Waste Package Transporter indicates that the vehicle will be a moderately complex system. Significantly more design work will be required to determine the exact I/O requirements. Focused analyses on several of the sub-systems identified in the I/O list are recommended.

6.9 WASTE EMPLACEMENT DATA COMMUNICATION

This section will discuss the interface to the MGR OMCS and the relevance of this system in the waste emplacement process.

The OMCS provides supervisory control, monitoring, and selected remote control of primary and secondary repository operations. Primary repository operations consist of both surface and subsurface activities relating to waste receipt, preparation, and emplacement. Secondary repository operations consist of support operations for waste handling and waste treatment, utilities, subsurface construction, and Balance-of-Plant activities. Remote control of subsurface operations is the direct responsibility of this system. The system provides repository operational information, alarm capability, and human operator response messages during normal and emergency response situations. The system also has the ability to place equipment systems and utilities in a safe operational mode during emergency response situations. The OMCS provides data communications, data processing, managerial reports, data storage, and data analysis. Refer to Figure 10 for a graphical presentation of the interfaces between systems involved in the waste emplacement process.

6.9.1 Operator Interfaces and Control Stations

All of the devices for transmission of the emplacement process data will be networked together and will allow personnel on the surface to remotely operate the waste emplacement equipment. It is anticipated that the OMCS command center will consist of a control room from which all subsurface operations will be monitored and controlled. This control room will be equipped with engineering workstations, mainframes, and graphics terminals that will provide the operators with direct real-time data. Sufficient storage capacity should exist for time-stamping the data as it is received. This control room will also have a large, wall-sized mimic board so operators can immediately gain insight as to what is occurring underground. The network can be installed with sufficient access points underground to allow an authorized individual to temporarily hook up a lap top or notebook computer and have access to the transmitted data and assume control of the emplacement equipment. Versatility, accuracy, timeliness, and robustness are all attributes that can be implemented in the OMCS to enhance the emplacement process.

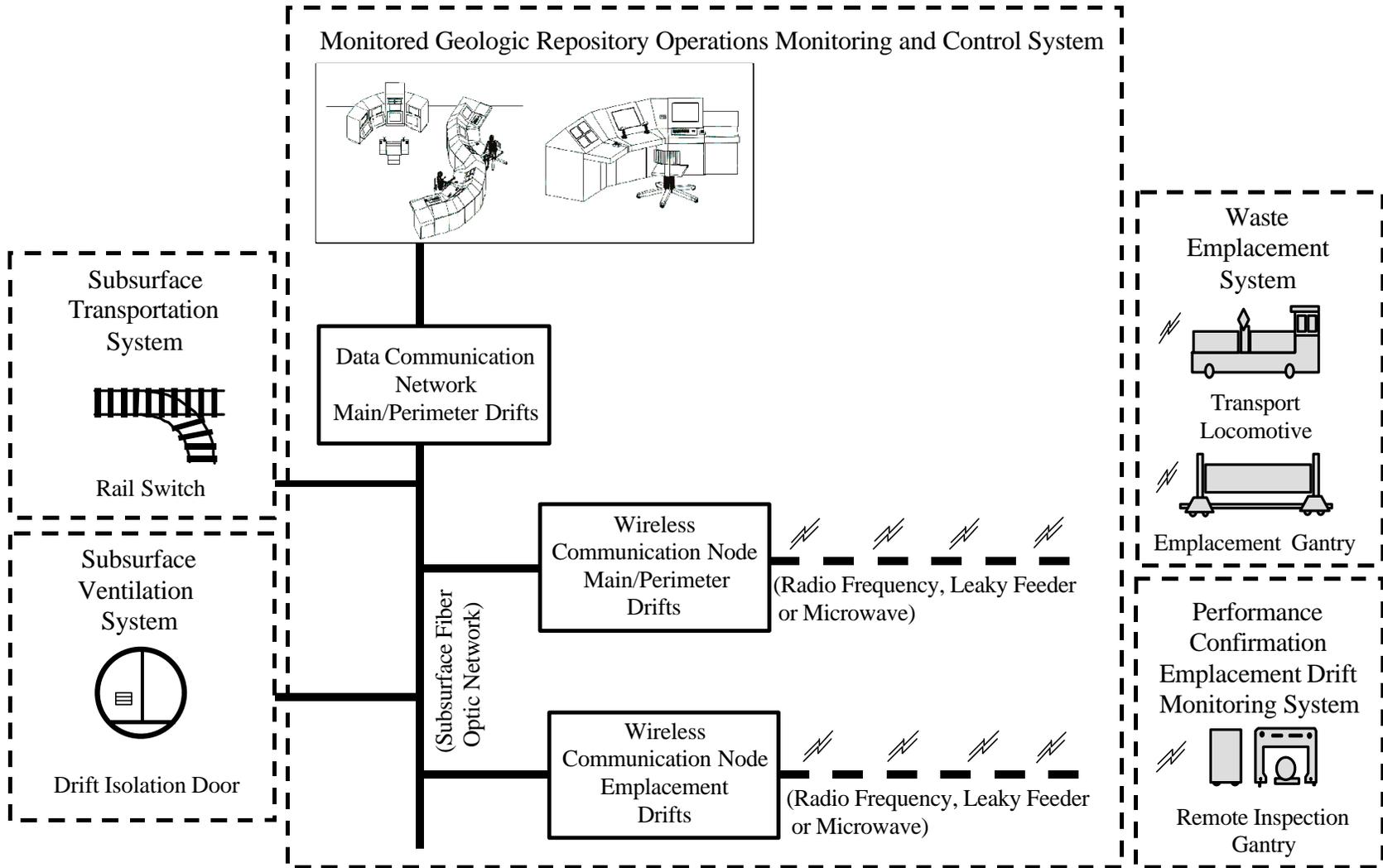


Figure 10. Operations Monitoring and Control System Interfaces

6.10 SAFETY AND RELIABILITY

This section discusses safety and reliability issues related to the design of the Waste Emplacement System. According to the most recent safety classification analysis (CRWMS M&O 1999a), some critical components of the Waste Emplacement System are currently designated with the safety classification of Quality-Level 1 (QL-1), which is the highest ranking. This includes components such as the Transport Locomotives, Waste Package Transporter, and Control and Tracking Systems. Failure of any of these system components could potentially have an adverse impact on public safety and on the repository's ability to isolate waste. Other components, such as the Emplacement Gantry are designated as QL-2, which means that a component failure could have an indirect adverse affect on public safety and/or adversely affect the operational safety of the potential repository. Given these safety classifications and the inherent consequences should key system components fail, this section outlines the issues and strategies related to designing a Waste Emplacement System that will meet both safety and reliability requirements.

A discussion of the preclosure I&C safety strategy is outlined in the *Monitored Geologic Repository Instrumentation and Control System Strategy* document (CRWMS M&O 1999b, section 4). The upper-level strategy includes: (1) designing the potential repository in such a way so as to minimize the number of SSCs important to radiological safety, (2) reducing facility operational risk (i.e., by developing systems that are robust and reliable), (3) emphasize use of proven technology, (4) where possible, employ passive safety features that minimize reliance on auxiliary support systems, and (5) identify design needs for system testing, construction, and operation. These strategies, and others, are addressed, preliminarily, in the following subsections.

6.10.1 Terminology and General Issues

This section outlines some of the general issues and terminology associated with developing a Waste Emplacement System that is both safe and reliable.

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." The reliability of a component or system varies with time. As indicated by its QL classification, the operational reliability of the locomotives, transporter, and gantry will need to be exceptionally high. This requirement, combined with the handling and transportation of massive loads, and operating under relatively harsh environmental conditions, are key drivers for developing a focused design effort to address reliability issues. As discussed below, several strategies are being considered.

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. To meet anticipated throughput requirements, the Waste Emplacement System will need to emplace, on average, about two WPs per day. This provides sufficient time for preparing, checking readiness, and servicing system components. This should result in high system availability for scheduled operations.

Designing for adequate availability will involve provisions for redundancy in subsystems and/or radiation hardening to withstand the environment, where deemed necessary, depending on the criticality that a given operation function without interruption during the mission time. A critical function is, for example, the ability to move the gantry while carrying a WP in the emplacement drift. This must be accomplished without a breakdown of the drive motors or associated control systems because maintainability (corrective maintenance) is more difficult inside the emplacement drift. In contrast, the failure of an environmental thermal sensor during the emplacement process might be deemed less critical. The design, therefore, might include redundancy in the motive and control systems, radiation shielding, and use of radiation and heat-resistant components in motors and electrical conductors.

The *maintainability* of a system is its ability to be retained in, or returned to, its designed operating state. The Waste Emplacement System will be designed to include frequent inspections, scheduled preventative maintenance, and on-board diagnostic functions. The capability for testing and calibration of system equipment shall be provided. As discussed below, the system will implement a defense-in-depth design strategy that will eliminate the risk of single-point failure. The Waste Emplacement System will be designed for accessibility to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment. System Reliability, Availability and Maintainability design issues related to the Waste Emplacement System are discussed further in the next subsection.

Designing for *defense-in-depth* is a strategy for developing highly reliable systems. Essentially, it involves eliminating single-point failures by designing in *redundant*, technically *diverse* and independent backup systems for critical system functions or components. Depending on the requirements for reliability, systems can be designed with two, three, and even four layers or modes of redundancy to defend against overall system failure. Added reliability also can come from employing diverse technologies or components in the construction of the system. For example, if redundant control computers are employed, the component can be obtained from two different manufacturers. This will provide added protection against common-mode failures. Additional system reliability can be obtained by *physical separation* of redundant components. This may include routing redundant communication cables on opposite sides of an emplacement vehicle.

Single-Point Failures are to be avoided in the design of safety-critical systems. This means that no one single failure can result in a system failing to perform a safety-critical function. Fault tree analyses and single-failure analyses should be performed to verify that no single failure in either the hardware or software will cause a failure that would cause the loss of a safety function. The single-failure analysis shall be performed in conjunction with comprehensive analysis of the failure modes and effects of the Waste Emplacement System.

Fault Tolerance is the ability of a system to respond gracefully to an unexpected hardware or software failure. There are many levels of fault tolerance, the lowest being the ability to continue operation in the event of communication or power failures. Many fault-tolerant systems employ two or more duplicate component systems, such that if one fails, the other can take over.

A *fail-safe operation* refers to a set of output states of a system that can be identified as being safe. The Waste Emplacement equipment should be designed to “fail safe” by ensuring that it defaults to these outputs in the event of failure or the inability to recover from failure. For example, this would include ensuring that loads are not dropped in the event of a power 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. In the case of the Emplacement Gantry, for example, the gantry could be designed such that if communications with the vehicle are lost, the gantry would assume a safe configuration and await re-establishment of communications.

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.

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

6.10.2 Waste Emplacement System Reliability, Availability, and Maintainability

As the design concepts for the emplacement system evolve and mature, it will be important to thoroughly evaluate the system’s reliability, availability, and maintainability (RAM) in accordance with the *Reliability, Availability, and Maintainability Plan* (YMP 1993). A formal, in-depth, “RAM analysis” of the emplacement system is, by itself, an extensive analytical undertaking and is outside the scope of this analysis. However, because of the importance of this topic to the overall success of the design and implementation of a remotely operated emplacement system, this section will briefly identify and outline RAM issues.

RAM analysis of the emplacement system will assess availability for various design concepts as the design evolves. Expressions for availability will be based on the SDD requirements and coordinated with a simulation code throughput modeling effort. The RAM analysis effort should use the guidelines provided in appropriate references such as the *Guidebook for Reliability, Availability, and Maintainability Analysis of NWTs Repository Equipment* (Orvis 1981), ANSI/IEEE Std 352-1987 *IEEE Guide for General Principles of Reliability Analysis of Nuclear Power Generating Station Safety Systems*, and ANSI/IEEE Std 577-1976 *IEEE Standard Requirements for Reliability Analysis in the Design and Operation of Safety Systems for Nuclear Power Generating Stations*. Quantitative system availability analyses are performed to determine if the SDD availability requirements are met.

In addition, the possibility of failures induced by human error needs to be addressed for its effect on reliability and availability. Human factors engineering of the operational control system,

preparation of clear procedures, and operator training will help to reduce the likelihood of such errors.

As follows, the principal subsystems of the Waste Emplacement System pose different RAM issues, depending on their role and criticality to mission success.

Gantry Mobility Subsystem—Loss of function to move the gantry on the track while in an emplacement drift is a critical issue. Failure of motors, gears, bearings, wheels, control computers, etc., could halt the operation. The critical issue for corrective maintenance is the ability to retrieve the gantry from an emplacement drift to permit hands-on repair. This might require use of a special retrieval gantry or other technique (bringing another emplacement gantry in to tow out the failed unit). Recovery from gantry derailment is a related but separate issue from RAM considerations for reliability and maintainability of the active locomotive subsystems. Reliability issues include environmentally enhanced failure rates for electrical insulation, motor windings, bearings and lubricants, etc. Reliability-centered maintenance should be applied to determine the optimal test and/or refurbishment program for the control system.

Vehicle Control System—The criticality for loss of function of the control systems is essentially the same as for the locomotive system plus the additional concern that some failure modes might lead to a “runaway” situation, e.g., where the gantry would drive at maximum speed until mechanical stops installed on the track are hit. There would appear to be less criticality for failure of the sensor control subsystem since the gantry should be able to be driven out of a drift to permit repair.

Prioritization of the RAM requirements for the sensor control subsystem (as for the sensors themselves) is an issue of the criticality of mission success for a given measurement. Reliability issues include environmentally induced failures of electronic and computer circuitry, spurious signals from ionizing radiation, insulation breakdown, etc. In addition, radiation hardening and shielding may be applied to reduce the environmental effects. Reliability-centered maintenance should be applied to determine the optimal test and/or refurbishment program for the control system.

I&C for the Waste Emplacement System will be based on digital computer technology. As the monitoring and control of these systems would take 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 Waste Emplacement Control System at Yucca Mountain. Therefore, it is recommended that IEEE Std 603-1998 *IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations* and IEEE Std 7-4.3.2-1993 *IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations* be consulted to establish the functional and design requirements for the computer-based components of the Waste Emplacement System. These two standards have been endorsed by the NRC in Regulatory Guide 1.152 *Criteria for Digital Computers in Safety Systems of Nuclear Power Plants* and Regulatory Guide 1.153 *Criteria for Safety Systems*.

Communication System—Failure of the communication system is similar to that of the control system. The portions of the communication system that are mounted on the gantry are subject to the same issues as described above for the control system, since such failures may result in loss of external control to drive the gantry back out of the drift. Radiation, thermal hardening, and shielding should be included in the design to improve reliability. As necessary, redundancy and diversity can be designed into key components and circuitry. Alternatively, or in addition, the design can provide for easy removal and replacement of failed modules to permit quick return to the mission.

Key components of the communication equipment will be mounted outside the emplacement drift in a less hostile environment and will be accessible for maintenance. The components installed within the emplacement drifts, however, will require extensive consideration of long-term environmental effects and reliability.

Sensor System—The criticality of failure of one or more of the sensor subsystems depends on the criticality or urgency of obtaining a given data point at any given time because repair can be performed quite readily by driving the gantry out of the emplacement drift to the main drift where hands-on maintenance can be performed. Prioritization of the RAM requirements for the sensor subsystem is then an issue of the criticality of mission success for a given measurement. Sensors critical to gantry operations will each have redundant backup sensors and systems that will eliminate the possibility of single-point failures. Possible failures within the monitoring instrumentation packages and sensors, including the camera systems, environmental thermal and radiation sensing instruments, etc., will not jeopardize recovery of the gantry from inside the emplacement drift and, therefore, will not require redundancy in design.

Scheduled testing and preventative maintenance of the emplacement system can be conducted periodically in human-rated areas in the perimeter main drifts and at maintenance areas located at the surface. However, during the time the emplacement gantry is deployed inside an emplacement drift containing WPs, it will be inaccessible to personnel. Therefore, it is very important that the remote emplacement system work reliably. The consequences of a failed emplacement gantry inside an emplacement drift can be significant.

In general, the design must include provisions for preventive and corrective maintenance. It appears that corrective maintenance of the subsystems on the emplacement gantry can be performed in the main drifts or at maintenance facilities located at the surface, away from radiation and thermal hazards. Corrective maintenance of the subsystems on the locomotives and Waste Package Transporter can also be performed at maintenance facilities located at the surface. Depending on cost and logistical constraints, the subsystems might be designed for a remove-and-replace maintenance philosophy. The design would accommodate ease of access with connectors and fasteners to facilitate repair. Components so removed would be refurbished for reuse or discarded.

In general, the maintainability provisions for the drive and control subsystems will assume preventive maintenance in accord with the reliability analysis. That is, periodic testing and refurbishment, using the principles of reliability-centered maintenance will be applied to assure a suitably low probability of failure during the mission time. Nevertheless, the design must also

include provision for rescue of a failed emplacement gantry from an emplacement drift. How to accomplish this will be the subject for future analysis.

The primary constraints for maintainability of the emplacement systems are the high radiation levels and the temperature in the emplacement drifts and the occasionally elevated radiation levels in the turnouts that would pose a high hazard to humans should there be a need to repair or rescue either a gantry or locomotive after a breakdown. In addition, space limitations in the emplacement drift and turnouts may impede any maintenance operations.

A rigorous RAM analysis program for the Waste Emplacement System is needed. It will need to support the selection among design alternatives and support optimization of design for cost versus throughput (consistent with SDD requirements) for the required maintainable service life. The analysis should address issues such as:

- Random failure, inherent to particular sensors, mechanisms, etc.
- Environmental effects on failure rates
- Human exposure issues on maintenance activities; need for auxiliary shielding and/or cooling
- Preventive maintenance and reliability-centered maintenance concept applications
- Human reliability analysis during operations and maintenance, installation, configuring for specific missions
- Maintenance philosophy for various subsystems
- Repairability/accessibility of various failure modes of each subsystem
- Logistic and spare-parts support program
- Throughput and availability requirements
- Likelihood and impact of DBEs

The *Guidebook for Reliability, Availability, and Maintainability Analysis of NWTS Repository Equipment* (Orvis 1981) developed guidelines for establishing a RAM program for a prior concept for mined geologic disposal of high-level nuclear wastes. The guidebook provides instructions for applying both qualitative and quantitative methodologies for RAM analysis and design support. Although it was developed for earlier phases of the Project, the techniques for defining, prioritizing, and analyzing RAM elements remain relevant.

Depending on the level of RAM effort defined for a given unit, the program may apply one or more of the following:

- RAM Checklists (including Reliability Checklist and Maintainability Checklist)

- Failure Mode and Effects Analysis (or a variant such as Failure Modes, Effects and Criticality Analysis)
- Reliability Block Diagrams
- Maintainability Evaluation (e.g., estimates of access times, repair times, radiation exposure of workers, etc.)
- Fault Tree Analysis for detailed reliability analysis of subsystems and systems
- Event Tree Analysis to define RAM related scenarios
- Failure rate data

Except for the checklists, which are qualitative, the other techniques can be applied both qualitatively and quantitatively. The qualitative application of failure mode and effects analysis, reliability block diagrams, fault tree analysis, and event tree analysis provides a structured technique for examining how and why a mission may fail or why a failure may be critical. The quantitative application of these techniques can help in the optimization of cost versus performance. If deemed appropriate, operation of the emplacement system can be modeled in a simulation.

To support a quantitative analysis, including simulation, the RAM program must also include development of a database. Failure-rate data for repository-specific components and equipment has to be developed. Where no present data exist for the specific environment or duty, data synthesis and estimates must be developed. Development of operational engineering models and prototypes may be helpful in obtaining improved system reliability information. Environmental effects of radiation and temperature on failure rates must be included.

7. CONCLUSIONS

This document incorporates recent design concepts for major components of the Waste Emplacement System, including the Transport Locomotives, Waste Package Transporter, and Emplacement Gantry. This document reviewed possible impacts of changes to the repository design due to the recent License Application Design (LADS) effort and activities associated with selecting the Enhanced Design Alternatives (EDA) (CRWMS M&O 1999f, Stroupe 2000). As indicated in Section 6.3, the direct impacts on the basic control system design strategy and approach were considered to be minor.

This document is consistent with the guidance contained in the *Technical Guidance Document for License Application Preparation* (YMP 1999b). Applicable requirements associated with interim licensing guidance and the *Monitored Geologic Repository Requirements Document* (YMP 1999a) are allocated to the *Waste Emplacement/Retrieval System Description Document* (CRWMS M&O 2000e, section 1.2), which in turn is the primary source of criteria and requirements for this analysis (see Section 4.2).

This document may be affected by technical product input information that requires confirmation. Any changes to the document that may occur as a result of completing the confirmation activities will be reflected in subsequent revisions. The status of the input information quality may be confirmed by review of the Document Input Reference System Database (DIRS). Within this document there is one TBD (TBD-406) associated with input Criterion 4.2.3. The resolution of this TBD does not impact the conclusions or output of this document because this analysis supports the general concept of achieving ALARA occupational radiation exposure levels rather than addressing specific yet to be determined quantitative program goals.

The following paragraphs provide a brief summary of the material covered and design criteria used within this document and highlights the key results and recommendations.

Section 6.2 provides a general overview of waste emplacement concept-of-operations. The current emplacement concept utilizes remote monitoring and control and remote handling techniques extensively in order to minimize occupational radiation exposures to workers as stipulated in Criterion 4.2.3. This section summarizes current control strategies and methodologies for key phases of the waste emplacement process. The conclusions are that further analysis be conducted, similar to that outlined in NUREG/CR-3331, to formally allocate control functions to human or machine control. It recommends further analysis be conducted to characterize safety and performance risks associated with the waste emplacement process. Additional design analysis should also be performed to assess the feasibility and viability of increasing the level of automation in the waste emplacement process.

Section 6.3 evaluates the impact of LADS – EDA II design changes on the design of instrumentation and controls for waste emplacement. The conclusions of this evaluation are that the direct impacts on the basic control system design strategy and approach were relatively minor. The new waste package design emits higher levels of radiation which will lead to increased shielding on protective enclosures for sensitive electronics. The use of steel sets and wire mesh ground support, along with longer drift lengths, may impact in-drift wireless

communication system design. Section 6.3 also outlines advantages of using digital instrumentation and controls and indicates the suitability of using such technology in the development of the Waste Emplacement System. It discusses several design factors associated with developing digitally-based control systems for safety-related applications in a regulated nuclear environment (in support of Criteria 4.2.2 and 4.2.3 and guidelines in the TGD). It considers design factors such as the use of commercially available software and the need for software quality assurance, strategies to avoid potential common-mode failures, regulatory precedence and design issues, and the need to consider the overall systems aspects of developing digital control systems. It concludes that further design and development work is needed to address these important design factors in more detail.

Section 6.3 also concludes that criteria contained in the *Waste Emplacement/Retrieval System Description Document* (CRWMS M&O 2000e, section 1.2) should be revised and expanded to cover I&C requirements. In this SDD, there are references to steel, welds, and mechanical loads but virtually no mention of control communication, computers, software, instruments, sensors or human-machine interfaces. The Waste Emplacement and Retrieval Systems will be composed of on-board computers, radios, power supplies, instruments and sensors. The addition of a function similar to the following statement is suggested: “The Waste Emplacement System shall provide features for monitoring external environmental and operating conditions including visual, thermal and radiological conditions.” Note that this is a separate functional need than either Function 1.1.11 or 1.1.14. The system not only needs to “operate” within the natural and induced environmental condition but it also needs to monitor and report what those conditions are. Also, add corresponding criteria related to visual, thermal and radiological monitoring in the System Design Criteria section of the SDD. A criterion should also be added to provide design engineers guidance on the system reliability requirements.

Section 6.4 presents a functional architecture for the control system of the overall Waste Emplacement System. Functional block diagrams provide a top-down design perspective and map key Waste Emplacement functions found in the SDD to individual components and devices being designed to accomplish those functions. The functional block diagrams also identify key system interface points to other repository systems. The conclusion that can be derived from this section is that a functional architecture has been developed that adequately and logically accounts for the diverse systems and components necessary to satisfy waste emplacement design requirements.

Section 6.5 presents a physical architecture for the on-board control systems that enable remote operation of emplacement vehicles in a safe and reliable manner. The section presents a viable design for a vehicle control system that can be used as the basis for both the Emplacement Gantry and the Transport Locomotives. These initial design concepts begin to address Criteria 4.2.1, 4.2.2, 4.2.4, and 4.2.5. The control system design incorporates defense-in-depth design features, including the use of redundant backup systems, physical separation of backup components, and use of diverse I&C technologies. It is concluded that a control system based on readily available technologies such as PLCs and embedded microprocessors can be developed that would incorporate this defense-in-depth approach and provide adequate levels of system reliability. A redundant PLC based control system and supported by auxiliary on-board microprocessors is presented that is similar to those effectively used to remotely control transit

and freight locomotives, semi-automated mining equipment, and overhead gantry cranes. This technology is commercially available from multiple sources. A brief discussion of the vehicle control software and mobile communication systems was also presented. It is concluded that additional work should be performed to evaluate other possible control system configurations such as systems based on redundant distributed microprocessor or microcontroller systems.

As indicated in Section 6.5.4, the Waste Emplacement process will rely on a significant amount of software. An integrated software development program should address such things as: development methodology, development controls, product assurance and testing, precedence within regulatory approval processes, life-cycle operations, maintenance, and so forth. It is concluded that software development and design is a vital aspect of emplacement system design and that much more work is needed in the area. It is recommended that a future analysis examine how other safety-critical industries have addressed software development, reliability, and testing to achieve successful software-based control systems. It is also recommended that the work of preliminary software design be initiated and functional flow diagrams be produced. This would include researching and recommending possible development platforms and tools, real-time operating systems, real-time control issues, appropriate programming languages, relevant routines for error-checking, and reliability and testing strategies. It is also recommended that an in-depth review and study of the regulatory documents and standards associated with developing and testing reliable software be conducted.

Sections 6.6 through 6.8 present preliminary I&C design concepts for the Waste Emplacement Gantry, Gantry Carrier, Transport Locomotives, and Waste Package Transporter (in support of Criteria 4.2.1, 4.2.2, and 4.2.5). These sections also provide preliminary lists of the sensors, actuators and instrumentation to control and monitor each piece of emplacement equipment. Preliminary Control System I/O Lists are provided which give an initial estimate of the size and complexity of the I&C needed for each major piece of equipment used in the Waste Emplacement System.

Section 6.6 describes a viable control and configuration of the Emplacement Gantry. Several key component systems and interfaces were described, including: the locomotion and braking, control of the waste package hoisting mechanisms, vision systems, thermal monitoring and control, radiological monitoring systems, and on-board safety systems. It is concluded from this section that the Emplacement Gantry vehicle will require an integrated I&C system consisting of approximately 230 inputs and outputs. Section 6.6. also presents preliminary I&C design concepts for the Emplacement Gantry Carrier rail car. The Gantry Carrier will interface with the Transport Locomotives and have its own fail-safe braking systems.

Section 6.6 recommends a re-design of the Emplacement Gantry hoist mechanism to eliminate the possibility of single-point mechanical failures. The current design concept is vulnerable to jamming in the hoist mechanism. If one of the four ball-screws fails or becomes jammed, then the WP load could become stuck within the Gantry. There are a number of fault-tolerant and redundant drive design approaches that can be investigated and adapted for use in this application.

Section 6.7 presents preliminary I&C design concepts for the Transport Locomotives which will be used to haul waste packages from the Waste Handling Building into the subsurface repository. Several key component systems and interfaces were described, including: the locomotion and braking, rail car coupling systems, vision systems, thermal monitoring and control, radiological monitoring systems, and on-board safety systems. This section also describes control system interfaces between the Transport Locomotives and the Waste Package Transporter rail car. For safety and reliability reasons, two locomotives will be used in tandem, one fore and one aft, to escort the Waste Package Transporter up and down the north ramp within the repository. The Transport Locomotives will be designed for both manual and remote supervisory control. It is concluded from this section that the Transport Locomotives will require an integrated I&C system consisting of approximately 164 inputs and outputs.

Section 6.8 presents preliminary I&C design concepts for the Waste Package Transporter which will be used to transport waste packages within the human-rated main drifts of the repository. The Waste Package Transporter will be a highly shielded rail car to protect personnel from radiation. Due to the exceptionally large combined mass of the Transporter and waste package, a key aspect of the design is the redundant fail-safe braking system. In addition, the Transporter will include waste package loading mechanisms, internal and external vision systems, a thermal monitoring system, radiological monitoring systems, and mechanical, electrical, and data communication interfaces with the Transport Locomotives. It is concluded in this section that the Waste Package Transporter will require an integrated I&C system consisting of approximately 110 inputs and outputs.

Section 6.9 describes the data communication interfaces between the Waste Emplacement System and the MGR Operations Monitoring and Control System (in support of Criterion 4.2.5). This section describes how the waste emplacement equipment will be remotely controlled and monitored from a central control facility located at the surface. Monitoring and control information will be transmitted over a data communication network that is part of the MGR Operations Monitoring and Control System.

Section 6.10 discusses safety and reliability issues related to the design of the Waste Emplacement System. Recommendations for Reliability, Availability, and Maintainability (RAM) analyses and for a future RAM program have also been provided. This section begins to lay out the strategies and methods that will need to be developed to satisfy Criteria 4.2.2, 4.2.6 and 4.2.7.

The scope of this analysis focused on the instrumentation and controls for the Waste Emplacement System. In the course of developing this analysis several areas of work were identified that were beyond the scope of this document. It is recommended that additional design and analysis work be performed in the following areas:

1. Recommend developing an analysis that addresses the I&C aspects of recovery from off-normal operational events (derailment, failed or stuck emplacement equipment, etc.)
2. Recommend developing an analysis that focuses on the design of I&C for Waste Retrieval.

3. Recommend updating and revising preliminary Waste Emplacement System Process and Instrumentation Diagrams (P&IDs) to incorporate the most recent design changes.
4. Initiate a Technology Evaluation and Concept Testing Program that addresses the core technology needs of the Waste Emplacement System. These include mobile-remote communication, redundant computing and control systems, developing robust equipment for operation in adverse thermal and radiological conditions.

INTENTIONALLY LEFT BLANK

8. REFERENCES

8.1 DOCUMENTS CITED

Air Brake Association 1975. *Engineering Design of Railway Brake Systems*. Chicago, Illinois: Air Brake Association. TIC: 245141.

Air Brake Association 1998. *Management of Train Operation and Train Handling*. Chicago, Illinois: Air Brake Association. TIC: 245636.

CRWMS M&O (Civilian Radioactive Waste Management System Management and Operating Contractor) 1995. *Subsurface Repository Remote Handling & Robotics Evaluation Report*. BC0000000-01717-5705-00016 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19960402.0542.

CRWMS M&O 1996a. "Electronic Technologies & Design Strategies for Elevated Temperature Environments." Attachment I of *Preliminary Analysis of Remote Monitoring & Robotic Concepts for Performance Confirmation*. BCAI00000-01717-0200-00001 REV 00. Las Vegas, Nevada: CRWMS M&O. TIC: 240458.

CRWMS M&O 1996b. "Power & Communication Technologies for Remotely Operated Systems." Attachment III of *Preliminary Analysis of Remote Monitoring & Robotic Concepts for Performance Confirmation*. BCAI00000-01717-0200-00001 REV 00. Las Vegas, Nevada: CRWMS M&O. TIC: 240462.

CRWMS M&O 1996c. "Remotely Operated Vehicles." Attachment IV of *Preliminary Analysis of Remote Monitoring & Robotic Concepts for Performance Confirmation*. BCAI00000-01717-0200-00001 REV 00. Las Vegas, Nevada: CRWMS M&O. TIC: 240464.

CRWMS M&O 1996d. "Remote Manipulation, Inspection and Sensing Technologies for Hazardous Environments." Attachment V of *Preliminary Analysis of Remote Monitoring & Robotic Concepts for Performance Confirmation*. BCAI00000-01717-0200-00001 REV 00. Las Vegas, Nevada: CRWMS M&O. TIC: 240466.

CRWMS M&O 1997a. *Emplacement System Control and Communication Analysis*. BCA000000-01717-0200-00016 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19980113.0786.

CRWMS M&O 1997b. *Preliminary Analysis of Remote Monitoring & Robotic Concepts for Performance Confirmation*. BCAI00000-01717-0200-00001 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19990802.0325.

CRWMS M&O 1997c. *Repository Rail Electrification Analysis*. BCAC00000-01717-0200-00002 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19980122.0462.

CRWMS M&O 1997d. *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.

CRWMS M&O 1997e. *Performance Confirmation Data Acquisition System*. BCAI00000-01717-0200-00002 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19980513.0133.

CRWMS M&O 1998a. *Review of Safety-Related Data Communication Systems*. BC0000000-01717-0200-00019 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19980825.0156.

CRWMS M&O 1998b. *Repository Subsurface Control Integration Plan*. BCAC00000-01717-4600-00001 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19990223.0154.

CRWMS M&O 1998c. *Mobile Waste Handling Support Equipment*. BCAF00000-01717-0200-00006 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19980819.0397.

CRWMS M&O 1999a. *Classification of the MGR Waste Emplacement System*. ANL-WES-SE-000001 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19990927.0477.

CRWMS M&O 1999b. *Monitored Geologic Repository Instrumentation and Control System Strategy*. BA0000000-01717-5700-00023 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19990505.0448.

CRWMS M&O 1999c. *Waste Emplacement and Waste Retrieval – I20I2I24MA*. Activity Evaluation, September 22, 1999. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19991020.0135.

CRWMS M&O 1999d. *Review of NRC Approved Digital Control Systems Analysis*. ANL-OMC-CS-000001 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19991019.0477.

CRWMS M&O 1999e. *Subsurface Shielding-Specific Source Term Evaluation*. CAL-WER-NU-000001 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19990831.0053.

CRWMS M&O 1999f. *License Application Design Selection Report*. B00000000-01717-4600-00123 Rev 01. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.19990528.0303.

CRWMS M&O 2000a. *Subsurface Repository Integrated Control System Design*. ANL-MGR-CS-000001 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.20000321.0284.

CRWMS M&O 2000b. *Waste Package Transport and Transfer Alternatives*. ANL-WES-ME-000001 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.20000317.0261.

CRWMS M&O 2000c. *Bottom/Side Lift Gantry Conceptual Design*. ANL-WES-ME-000003 REV 01. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.20000420.0399.

CRWMS M&O 2000d. *Instrumentation and Controls for Waste Emplacement*. TDP-WES-CS-000001 REV 00. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.20000202.0168.

CRWMS M&O 2000e. *Waste Emplacement/Retrieval System Description Document*. SDD-WES-SE-000001 REV 00. Volume I. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.20000214.0302.

CRWMS M&O 2000f. *Instrumentation and Controls for Waste Emplacement*. Development Plan TDP-WES-CS-000001 REV 00 ICN 01. Las Vegas, Nevada: CRWMS M&O. ACC: MOL.20000630.0245.

DOE (U.S. Department of Energy) 2000. *Quality Assurance Requirements and Description*. DOE/RW-0333P, Rev. 9. Washington, D.C.: U.S. Department of Energy, Office of Civilian Radioactive Waste Management. ACC: MOL.19991028.0012.

Dyer, J.R. 1999. "Revised Interim Guidance Pending Issuance of New U.S. Nuclear Regulatory Commission (NRC) Regulations (Revision 01, July 22, 1999), for Yucca Mountain, Nevada." Letter from J.R. Dyer (DOE/YMSCO) to Dr. D.R. Wilkins (CRWMS M&O), September 3, 1999, OL&RC:SB-1714, with enclosure, "Interim Guidance Pending Issuance of New NRC Regulations for Yucca Mountain (Revision 01)." ACC: MOL.19990910.0079.

Hustrulid, W.A. ed. 1982. *Underground Mining Methods Handbook*. New York, New York: Society of Mining Engineers. TIC: 206655.

National Research Council 1997. *Digital Instrumentation and Control Systems in Nuclear Power Plants, Safety and Reliability Issues*. Washington, D.C.: National Academy Press. TIC: 235537.

Orvis, D.D.; Frank M.V.; Jacobsen, F.K.; and Clarke, W.M. 1981. *Guidebook for Reliability, Availability, and Maintainability Analysis of NWTs Repository Equipment*. ONWI-334. Columbus, Ohio: Battelle Memorial Institute, Office of Nuclear Waste Isolation. TIC: 223671.

Stroupe, E.P. 2000. "Approach to Implementing the Site Recommendation Design Baseline." Interoffice correspondence from E. P. Stroupe (CRWMS M&O) to Dr. D.R. Wilkins, January 26, 2000, LV.RSO.EPS.1/00-004, with attachment. ACC: MOL.20000214.0480.

YMP (Yucca Mountain Project) 1993. *Reliability, Availability, and Maintainability Plan*. YMP/93-15 REV 0. Las Vegas, Nevada: Yucca Mountain Site Characterization Office. ACC: NNA.19940302.0081.

YMP 1999a. *Monitored Geologic Repository Requirements Document*. YMP/CM-0025, Rev. 3, DCN 01. Las Vegas, Nevada: Yucca Mountain Site Characterization Office. ACC: MOL.19990429.0228.

YMP 1999b. *Technical Guidance Document for License Application Preparation*. YMP/97-03, Revision 1. Las Vegas, Nevada: Yucca Mountain Site Characterization Office. ACC: MOL.19991025.0118.

8.2 CODES, STANDARDS, REGULATIONS, AND PROCEDURES

ANSI/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. TIC: 246332.

ANSI/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. TIC: 242994.

ANSI/IEEE Std 1008-1987. *IEEE Standard for Software Unit Testing*. New York, New York: The Institute of Electrical and Electronics Engineers. TIC: 237528.

AP-3.10Q, *Analyses and Models*. Rev. 2, ICN 0. Washington D.C.: U.S. Department of Energy, Office of Civilian Radioactive Waste Management. ACC: MOL.20000217.0246.

AP-SV.1Q, *Control of the Electronic Management of Data*. Rev. 0, ICN 1. Washington D.C.: U.S. Department of Energy, Office of Civilian Radioactive Waste Management. ACC: MOL.20000512.0068.

IEEE Std 7-4.3.2-1993. *IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations*. New York, New York: The Institute of Electrical and Electronics Engineers. TIC: 226866.

IEEE Std 379-1994. *IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems*. New York, New York: The Institute of Electrical and Electronics Engineers. TIC: 241086.

IEEE Std 603-1998. *IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations*. New York, New York: The Institute of Electrical and Electronics Engineers. TIC: 242993.

IEEE Std 730-1998. *IEEE Standard for Software Quality Assurance Plans*. New York, New York: The Institute of Electrical and Electronics Engineers. TIC: 246411.

IEEE Std 828-1998. 1998. *IEEE Standard for Software Configuration Management Plans*. New York, New York: The Institute of Electrical and Electronics Engineers. TIC: 247962.

IEEE Std 829-1998. 1998. *IEEE Standard for Software Test Documentation*. New York, New York: The Institute of Electrical and Electronics Engineers. TIC: 247961.

IEEE 1028-1997. 1998. *IEEE Standard for Software Reviews*. New York, New York: The Institute of Electrical and Electronics Engineers. TIC: 242864.

Lawrence, J.D. and Persons, W.L. 1994. *Survey of Industry Methods for Producing Highly Reliable Software*. NUREG/CR-6278. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 241381.

Lawrence J.D. and Preckshot, G.G. 1994. *Design Factors for Safety-Critical Software*. NUREG/CR-6294. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 241587.

NRC (U.S. Nuclear Regulatory Commission) 1987. *Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants*. NUREG-0800. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 203894.

Preckshot, G.G. 1993. *Data Communications*. NUREG/CR-6082. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 236616.

Preckshot, G.G. and Scott, J.A. 1996. *A Proposed Acceptance Process for Commercial Off-the-Shelf (COTS) Software in Reactor Applications*. NUREG/CR-6421. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 236612.

Pulliam, R.; Price, H.E.; Bongarra, J.; Sawyer, C.R.; and Kisner, R.A. 1983. *A Methodology for Allocating Nuclear Power Plant Control Functions to Human or Automatic Control*. NUREG/CR-3331. Washington, D.C.: U.S. Nuclear Regulatory Commission. TIC: 222975.

QAP-2-0, *Conduct of Activities*. Rev. 5, ICN 1. Washington, D.C.: U.S. Department of Energy, Office of Civilian Radioactive Waste Management. ACC: MOL.19991109.0221.

QAP-2-3, *Classification of Permanent Items*. Rev.10, ICN 0. Washington D.C.: U.S. Department of Energy, Office of Civilian Radioactive Waste Management. ACC: MOL.19990316.0006.

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.

Regulatory Guide 1.153, Rev. 1. 1996. *Criteria for Safety Systems*. Washington, D.C.: U.S. Nuclear Regulatory Commission. Readily Available.

Regulatory Guide 8.8 Rev. 3. 1978. *Information Relevant to Ensuring that Occupational Radiation Exposures at Nuclear Power Stations will be as Low as is Reasonably Achievable*. Washington, D.C.: U.S. Nuclear Regulatory Commission. Readily Available.

INTENTIONALLY LEFT BLANK

9. ATTACHMENTS

Not used.