CRWMS/M&O

Design Analysis Cover Sheet*Complete only applicable items.*

①

QA: L

Page: 1 Of: 66

2. DESIGN ANALYSIS TITLE Emplacement System Control and Communication Analysis			
3. DOCUMENT IDENTIFIER (Including Rev. No.) BCA000000-01717-0200-00016 Rev 00			4. TOTAL PAGES 66
5. TOTAL ATTACHMENTS NONE		6. ATTACHMENT NUMBERS - NO. OF PAGES IN EACH N/A	
	Printed Name	Signature	Date
7. Originator	Douglas A. McAfee		9-18-97
	Norman T. Raczka		9-18-97
8. Checker	William C. French		9-18-97
9. Lead Design Engineer	Daniel G. McKenzie		9-18-97
10. Department Manager	Kaylan K. Bhattacharyya		9/19/97
11. REMARKS			
<p>1. Primary area of responsibility for the originators:</p> <p>A. Douglas A. McAfee - Coordinated overall preparation of analysis and was the primary author for the sections regarding the mobile emplacement equipment (sections 7.4, 7.5, 7.6, 7.7).</p> <p>B. Norman T. Raczka - Primary author for sections discussing Isolation door control, rail switch control, RAM, and the SCADA network sections 7.2, 7.3, 7.8, 7.9).</p> <p>2. Other contributors to the analysis:</p> <p>A. Dennis Markman - Provided input for sections 7.5, 7.6, and 7.7</p>			

Design Analysis Revision Record*Complete only applicable items.*

①

2. DESIGN ANALYSIS TITLE	
Emplacement System Control and Communication Analysis	
3. DOCUMENT IDENTIFIER (Including Rev. No.)	
BCA000000-01717-0200-00016 Rev 00	
4. Revision No.	5. Description of Revision
00	Initial Issue

TABLE OF CONTENTS

1. PURPOSE	5
2. QUALITY ASSURANCE	6
3. METHOD	6
4. DESIGN INPUTS	6
4.1 DESIGN PARAMETERS	7
4.2 CRITERIA	7
4.3 ASSUMPTIONS	8
4.4 CODES AND STANDARDS	9
5. REFERENCES	9
6. USE OF COMPUTER SOFTWARE	11
7. DESIGN ANALYSIS	12
7.1 Introduction	12
7.1.1 Digital Instrumentation & Controls	12
7.2 Isolation Door Control System	15
7.2.1 Single Isolation Door Control Constraints	17
7.2.2 Turnover Block Isolation Door Constraints	22
7.3 Rail Switch Control System	26
7.3.1 Single Rail Switch Control Constraints	26
7.3.2 Turnover Block Rail Switch Control Constraints	28
7.4 Remotely Operated Emplacement Vehicles	28
7.4.1 Mobile Vehicle Control System Architecture	29
7.4.2 Emplacement Vehicle Communication Systems	34
7.5 Emplacement Gantry System	34
7.5.1 Emplacement Gantry: Component Systems	35
7.5.2 Preliminary Emplacement Gantry Input/Output List	39
7.5.3 Emplacement Gantry Carrier	42
7.5.4 Emplacement Gantry Carrier Control Interfaces	44
7.6 Transport Locomotive	45
7.6.1 Transport Locomotive Control Functions	45
7.6.2 Interfaces between Primary and Secondary Transport Locomotives	48
7.6.3 Transport Locomotive Input/Output List	51
7.7 Waste Package Transporter	53
7.7.1 Preliminary Waste Package Transporter Input/Output List	55
7.8 Emplacement System Reliability, Availability, and Maintainability	57
7.8.1 RAM Issues Related to the Emplacement System	58
7.8.2 Recommendations for a Future RAM Program	59

TABLE OF CONTENTS (Continued)

7.9	Repository Supervisory Control and Data Acquisition (SCADA) Network	61
7.9.1	Network Overview	61
7.9.2	Operator Interfaces and Control Stations	62
7.9.3	Estimated Size and Complexity	62
8.	CONCLUSIONS	65
9.	ATTACHMENTS	66

1. PURPOSE

The purpose of this analysis is to review and refine key design concepts related to remote handling and control systems presently under consideration for use in the waste emplacement process at the potential subsurface nuclear waste repository at Yucca Mountain. This analysis will discuss the key design concepts of the control systems that may be utilized for remotely controlling the vehicles and equipment traveling to, as well as within, the emplacement drifts and also the stationary equipment such as drift isolation doors and rail switches.

The scope and primary objectives of this analysis are to:

- ◆ Identify and discuss viable design concepts for monitoring and controlling the operation of the emplacement drift isolation doors. (Presented in Section 7.2)
- ◆ Identify and discuss viable design concepts for monitoring and controlling the operation of the rail switches which can be used to direct the rail-based equipment. (Presented in Section 7.3)
- ◆ Identify and discuss the various methods for monitoring and controlling the operation of the mobile emplacement equipment such as the waste package (WP) transporter, the WP loading mechanism, the transport locomotives, and the emplacement gantry. (Presented in Sections 7.4, 7.5, 7.6 and 7.7)
- ◆ Identify and outline reliability, availability, and maintenance (RAM) issues for the remotely operated emplacement system. (Presented in Section 7.8)
- ◆ Discuss the implementation of a repository Supervisory Control and Data Acquisition (SCADA) network. (Presented in Section 7.9)
- ◆ Provide recommendations for the features and attributes of the remote handling and communication components of the emplacement system. (Presented in section 8)

This analysis will focus on the development of input/output (I/O) lists including the types of I/O, redundancy considerations, processor requirements, and data transfer rates for the control systems mentioned above. Attention will be placed on operability, maintainability, and reliability for remote systems in a subsurface operating environment with control and communication equipment exposure to high temperatures and radiation. However, at this point in the design, specific reliability requirements for individual systems have not yet been determined or established.

As this analysis is an effort to establish the basic elements of a preferred emplacement concept for control and communication systems, the topics of off-normal and failure event recovery, as well as the response to design basis events (DBEs) are not addressed fully within this document but will be addressed in subsequent design analyses.

2. QUALITY ASSURANCE

The quality assurance classification of repository systems, structures and components has not yet been performed in accordance with QAP-2-3, *Classification of Permanent Items*. However, the emplacement process control and communication equipment are on the *Q-List* (Reference 5.1) by DOE direct inclusion covered under the classification item *Underground Service and Utility Systems*.

This design analysis activity has been evaluated in accordance with QAP-2-0, *Conduct of Activities*, (Reference 5.29) and has been determined to be quality affecting and subject to the requirements of the *Quality Assurance Requirements and Description* (QARD)(Reference 5.2). This design analysis is subject to quality assurance controls in accordance with NLP-3-18, *Documentation of QA Controls on Drawings, Specifications, Design Analyses, and Technical Documents*.

The output from this design analysis will not be used for procurement, fabrication, or construction and therefore the formal to-be verified (TBV) and to-be-determined (TBD) tracking system identified in QAP-3-9 is not applicable in accordance with NLP-3-15.

3. METHOD

The method used in this design analysis consists of identifying control system and communication characteristics and features, evaluating the technological alternatives, and selecting one or more choices from among the several competing technologies. This analysis is an effort to examine issues and develop concepts related to remotely controlling the waste package equipment in support of the emplacement operation. As such, the methodology of this analysis combines systems engineering approaches that include normative synthesis (a study of input documents for objectives and policies that are seen as desirable to the attainment of the objective), descriptive identification of existing systems and technologies, and scenario writing to aid in the formulation, discussion and preliminary analysis of key issues and ideas related to controlling and monitoring the emplacement operation. The general approach in developing this analysis is to: a) identify and review the key design input source documents, b) perform preliminary analyses and design activities, and c) summarize key findings and d) provide recommendations.

4. DESIGN INPUTS

This analysis is an early effort to develop remote handling concepts for waste package emplacement operations and therefore many of the source documents and resources, such as technical papers, vendor publications, and literature searches, will not be qualified design inputs. Since many of the inputs are unqualified, the outputs are unqualified and may not be used for procurement, fabrication, or construction. The unqualified inputs from the sources stated above are identified as TBV in this section.

4.1 DESIGN PARAMETERS

- 4.1.1** Based on the values obtained from Reference 5.6, Table 7.7-3, page 96, the maximum WP surface dose rate is estimated to be approximately 37.99 rem/hr.

4.2 CRITERIA

The following design criteria were developed to respond to Repository Design Requirements document (RDRD)(Reference 5.3) requirements that specifically apply to this design analysis. RDRD requirements are cited for each criteria statement.

- 4.2.1** The design and implementation of a remote control system for emplacement operations will enhance the safety of workers by allowing the operators to be removed from the dust, heat, radiation and inherent dangers of an underground operation. (RDRD 3.3.6.2.A, 3.3.6.3.F)
- 4.2.2** The design and implementation of a remote control system for emplacement operations will limit radiation exposure to humans and allow compliance with as low as is reasonably achievable (ALARA) guidelines for occupational doses. (RDRD 3.2.2.1.A, 3.2.2.1.B, 3.2.4.5.2, 3.7.3.7.A)
- 4.2.3** The remote control system will be designed with redundant features and self-diagnostic capabilities so that overall reliability of the system will be enhanced under all operating conditions. (RDRD 3.2.5.1, 3.2.5.1.4.A, 3.2.5.1.4.B, 3.2.5.1.5, 3.2.5.2.5.A, 3.5.1.1.1.C)
- 4.2.4** The remote control system will be designed for at least a 100-year maintainable life. (RDRD 3.2.5.4)(TBV)
- 4.2.5** The remote control system shall be equipped with suitable backup power supply to ensure operability of essential functions during loss of the primary electric power circuit. (RDRD 3.3.6.11.B)
- 4.2.6** A remote control and data communication backbone shall be installed in the repository to facilitate maintainable and reliable remote control of subsurface activities from surface locations. (RDRD 3.7.3.4.A.4)
- 4.2.7** The WP emplacement control system design shall include explosion and fire detection alarm systems and appropriate suppression systems with sufficient capacity and capability to reduce the adverse effects of fires and explosions on systems, structures, and components (SSCs) important to safety. (RDRD 3.2.1.7.A)
- 4.2.8** The SSCs important to safety shall be designed to perform their safety functions during and after credible fires or explosions in the underground repository. (RDRD 3.2.1.7.C)

4.2.9 Visual and audible alarm systems shall be provided to alert workers if radiation levels exceed established design levels. (RDRD 3.2.2.4.C)

4.2.10 The portion of the design of the WP emplacement control system that is important to safety shall include redundant systems to the extent necessary to maintain, with adequate capacity, the ability to perform safety functions. (RDRD 3.2.5.1.4.B)

4.2.11 The WP emplacement control system shall be designed to have adequate reliability to allow the repository to meet the throughput requirements identified in the Waste Delivery Schedule and its mission. (RDRD 3.2.5.1.5) (TBV)

4.3 ASSUMPTIONS

4.3.1 No human entry is planned in the emplacement drifts while waste packages are present. The waste emplacement/retrieval equipment may use robotics and/or remote control features to perform operations and monitoring within the emplacement drifts. Under off-normal conditions, human entry will be considered if protection to the workers can be provided. This assumption is Key 013 of the Controlled Design Assumption (CDA)(Reference 5.4). This assumption is used throughout this analysis. (TBV)

4.3.2 Waste packages will be placed center in-drift, on pedestals, using gantry emplacement. This assumption is based on Key 066 of the Controlled Design Assumption (CDA)(Reference 5.4). This assumption is used throughout this analysis. (TBV)

4.3.3 Not used.

4.3.4 Maximum allowable air temperature in emplacement drifts during:
Emplacement: 50° C dry-bulb, only in portion requiring access (TBV)
Retrieval: 50° C dry-bulb, only in portion requiring access (TBV)
(all Reference 5.4; DCSS 019)
This assumption is used in Section 7.4.1.2 of this analysis.

4.3.5 Rail transport will be used for subsurface transport of waste packages. This assumption is Key 010 of the Controlled Design Assumption (CDA)(Reference 5.4). This assumption is used in section 7.3 of this analysis. (TBV)

4.4 CODES AND STANDARDS

4.4.1 National Fire Protection Agency (NFPA)

NFPA 70/1996

National Electrical Code

4.4.2 University of California Research Laboratory (UCRL)

UCRL 15673

Human Factors Design Guidelines for
Maintainability of Department of Energy
Nuclear Facilities, June 18, 1985

4.4.3 U.S. Department of Defense (DOD)

MIL-STD-1472D

Human Engineering Design Criteria for
Military Systems, Equipment, and Facilities,
March 14, 1989

4.4.4 U.S. Department of Energy (DOE)

DOE Order 6430.1A

General Design Criteria, April 6, 1989

5. REFERENCES

- 5.1 U.S. Department of Energy, "*Q-List*", YMP/90-55Q, Rev. 04
- 5.2 U.S. Department of Energy, "*Quality Assurance Requirements and Description*", DOE/RW-0333P, Rev. 7
- 5.3 U.S. Department of Energy, "*Repository Design Requirements Document*" (RDRD), YMP/CM-0023, Rev. 0, ICN 1
- 5.4 CRWMS M&O, "*Controlled Design Assumptions Document*", DI# B00000000-01717-4600-00032 Rev. 04, ICN 02
- 5.5 CRWMS M&O, "*Mined Geologic Disposal System Advanced Conceptual Design Report*", DI# B00000000-01717-5705-00027 Rev 00
- 5.6 CRWMS M&O, "*MGDS Subsurface Radiation Shielding Analysis*", DI# BCAE00000-01717-0200-00001 Rev. 00
- 5.7 CRWMS M&O, "*Subsurface Waste Package Handling - Remote Control and Data Communication Analysis*", DI# BCA000000-01717-0200-00004 Rev 00

- 5.8 Committee on Application of Digital Instrumentation and Control Systems to Nuclear Power Plant Operations and Safety, *"Digital Instrumentation and Control Systems in Nuclear Power Plants, Safety and Reliability Issues"*, National Academy Press, 1997
- 5.9 Allen-Bradley Co. Inc., *"Industrial Control"*, Catalog Number 110, 1992
- 5.10 Allen-Bradley Co. Inc., *"Automation Systems"*, Publication B112, March 1997
- 5.11 CRWMS M&O, *"Repository Rail Electrification Analysis"*, DI# BCAC000000-01717-0200-00002, Rev. 00
- 5.12 CRWMS M&O, *"Preliminary Analysis of Remote Monitoring & Robotic Concepts for Performance Confirmation"*, DI# BCAI000000-01717-0200-00001 Rev 00
- 5.13 CRWMS M&O, *"Subsurface Repository Remote Handling & Robotics Evaluation Report"*, DI# BC00000000-01717-5705-00016, Rev. 00
- 5.14 Colorado School of Mines, Editor: L. Ozdemir, K. Hanna, *"Proceedings for the Third International Symposium on Mine Mechanization and Automation"*, Volume I & Volume II, June 12-14, 1995, Golden, Colorado
- 5.15 Martino, Silvio, *"Mining Locomotive Automation for the 90's"*, Goodman Equipment, 1995
- 5.16 CRWMS M&O, *"Performance Confirmation Data Acquisition System"*, DI# BCAI000000-01717-0200-00002 Rev 00
- 5.17 Telemotive Industrial Controls, *"Moving the World With Radio Remote Control"*, September, 1993
- 5.18 Electromotive Systems, Inc., *"Impulse Series 2"*, Brochure No. GVGS2-96A, 1996
- 5.19 CRWMS M&O, *"Evaluation of Waste Package Transport and Emplacement Equipment"*, DI# BCAF000000-01717-0200-00002 Rev 00
- 5.20 CRWMS M&O, *Yucca Mountain Site Characterization Project Reliability, Availability, and Maintainability Plan*, Rev 00, November 1993
- 5.21 D.D. Orvis, et al., *Guidebook for Reliability, Availability, and Maintainability Analysis of NWTS Repository Equipment*, Office of Nuclear Waste Isolation, ONWI-334, April 1981
- 5.22 B. S. Blanchard, et al., *Systems Engineering and Analysis*, Prentice Hall, 1990
- 5.23 Kessler, G. C. and Train, D. A., *Metropolitan Area Networks Concepts, Standards, and Services*, McGraw-Hill, 1992

- 5.24 Held, Gilbert, *"Internetworking LAN's and WAN's"*, John Wiley & Sons, 1993
- 5.25 DePatie, J.; Quandt, B.; Roy, B.; Saccente, C.; *"MPEG: The Big Squeeze"*, March 1, 1996
- 5.26 CRWMS M&O, *"Preliminary Waste Package Transport and Emplacement Equipment Design"*, DI# BCA000000-01717-0200-00012 Rev 00
- 5.27 Buckeridge, R.M., Carey, W.T., Graham, A.H., Martino, S.M., Reese, C.D., *"Rail Haulage Systems"*, Underground Mining Methods Handbook, Published by the Society of Mining Engineers, Inc.
- 5.28 CRWMS M&O, *"Subsurface Construction and Development Analysis"*, DI# BCA000000-01717-0200-00004 Rev 00
- 5.29 CRWMS M&O, Activity Evaluation, *"Waste Package Transport and Emplacement Equipment, Design Analysis (Summary Acct.: TR47FB6)"*, September 8, 1997
- 5.30 ANSI/IEEE, *"Standard Application of the Single-Failure Criterion to Nuclear Generating Station Safety Systems"*, Standard 379-1994, 16 pages, 1-55937-454-3.

6. USE OF COMPUTER SOFTWARE

Not Used

7. DESIGN ANALYSIS

7.1 Introduction

A recent design analysis entitled: *Subsurface Waste Package Handling - Remote Control and Data Communication*, issued in February of 1997 (Reference 5.7), has determined that the transport locomotives, the emplacement gantry, the waste package transporter, the emplacement drift isolation doors, and the rail switches all should be provided with remote control capability. This analysis is a refinement of the issues addressed in reference 5.7 and deals more specifically with the on-board control systems that may be used for the emplacement equipment.

7.1.1 Digital Instrumentation & Controls

The National Research Council, at the request of the Nuclear Regulatory Commission, recently conducted a landmark study and appraisal of the use of "Digital Instrumentation and Control Systems in Nuclear Power Plants" (Reference 5.8). In the report, the National Research Council indicates that the control systems in use today throughout the nuclear power industry were 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 difficult process.

It is important to note that the control systems currently being developed for the repository are based on digital instrumentation and control (I&C) technology. It is also important to note that the use of digital I&C technology does not currently have an extensive precedence within the Nuclear Regulatory Commission's licensing and approval processes.

There are several important advantages in the use of digital instrumentation and control systems 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 improved 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; 6) since there has been a wholesale shift to digital systems in virtually all other commercial sectors, digital systems are more widely available and implemented resulting in component obsolescence and waning vendor support for analog systems; 7) digital systems provide the potential 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 the nuclear waste repository.

The National Research Council's report also identified 6 technical areas and 2 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 Instrumentation and Control
- ◆ 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

And the strategic/programmatic issues are:

- ◆ Case-by-Case Licensing Process
- ◆ Adequacy of [the Nuclear Regulatory Commission's] Technical Infrastructure

All eight of these issues are important to consider in the design and development of repository control systems. Four of the eight issues identified above generally fall within the scope of this analysis and are discussed herein, at least preliminarily. The four issues not addressed in this analysis should be included in future analyses prepared regarding the control issue.

It should also be noted that the Nuclear Regulatory Commission has developed an extensive and valuable series of reports, designated the "NUREG-series" (NUclear REGulatory), that provide guidance for meeting regulatory requirements such as those contained in the Code of Federal Regulations. Frequently the NUREG's identify or incorporate national codes and standards developed by professional societies that are applicable in developing systems for use within the civilian nuclear industry. A formal review the NUREG library and determination of applicability of individual NUREGs will be conducted in separate analysis.

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 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.

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. These include: surface waste handling system, the subsurface ventilation system, power distribution system, repository environmental (temperature, humidity) monitoring, radiation monitoring systems, fire detection and suppression systems, personnel & process monitoring systems, emergency response and security and access control systems, warning and alarm systems, and so forth. 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. Far more work in this important area will be needed as the design progresses and matures.

Software Quality Assurance: An important element of the design, not encountered in the older analog technology, is the use and reliance on system software. Digital I&C systems rely on software programs to provide important aspects of the 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.

Based on the QARD, Supplement I, the OCRWM M&O has implemented two Quality Administrative Procedures (QAPs) that relate to the use and development of engineering and scientific software for design and analysis activities. QAP-SI-0 relates to the qualification process for engineering and scientific software to be used as controlled sources of information in the design process, with particular focus on the verification and validation (V&V) of software. QAP-SI-3 relates to configuration management of software to be used for design or analysis activities and involves assigning identification numbers to individual (i.e. discrete) software products.

The process of designing control software to operate, monitor and control emplacement systems within the repository may require years of development. It may be a significant period of time before discrete software products are produced that are appropriate for either the software V&V process, or to be assigned to the configuration management process. Prior to the application of the software related QAPs cited above, software quality assurance activities will need to focus on developing high level planning documents that outline the overall development, management, testing and product 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 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: Common-mode failures are failures in which a single error or problem disables multiple, independent system functions. An example of this would 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, incorporation of fault tolerance design features, and so forth. As indicated throughout this analysis, these design approaches are used when the potential consequences or costs of a failure would be considered unacceptable. The determination of which specific systems or components will, or will not need these higher levels of reliability and availability will be the subject of future analyses. Section 7.9 of this analysis also provides an additional, brief, discussion of these issues. There are also a number of standards available, such as ANSI/IEEE-379 (Reference 5.30) and similar standards, that have been developed for use in the nuclear industry which may be applicable and provide guidance in assessing single-failure criterion.

Dedication of Commercial Off-the-Shelf Hardware and Software: As indicated in reference 5.8, 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 Nuclear Regulatory Commission (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.

This 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.

7.2 Isolation Door Control System

After emplacement of waste begins, both development and emplacement activities will occur concurrently underground. Prior to emplacement of waste, underground work is referred to as *construction*. Once emplacement starts, subsurface construction is referred to as *development*. Emplacement and development activities will be separated, and dedicated emplacement and development crews will perform the respective work. With the exception of emergency or special, prearranged situations, the respective work crews will have no direct contact underground, and substantial isolation air locks will physically separate the emplacement and development activities. Development activities will be conducted by underground workers and other individuals trained in subsurface excavation. Their separation from the emplacement activities will isolate them from the radiation hazards present on the emplacement side of the repository. Emplacement activities will be conducted by workers experienced in nuclear safety, remote handling, and the special hazards associated with managing radioactive materials.

The construction and development of the repository will be completed in a series of blocks (also called panels) of emplacement drifts, with each panel consisting of between 5 and 22 emplacement drifts (Reference 5.28). Figure 7.2-1 shows the proposed sequence of emplacement drift development. The increments will allow completion of the repository in phases and the subsequent turnover to emplacement operations of drifts that are ready to receive waste packages. The current development concept involves relocating the isolation airlocks as blocks or panels of emplacement drifts are determined to be ready to receive waste packages. The varying number of drifts to be turned over to emplacement operations should be taken into account in the control system design for the stationary emplacement equipment. This analysis will base the initial design of the isolation door and rail switch control systems on the size of blocks to be turned over. The exact size of the blocks could vary with minimal effect on the final control system design.

The following sections will involve: 1) discussing a single isolation door and its operation, and 2) discussing the isolation door control system design and its accommodation of the drift turnover sequence.

FIGURE 7.2-1
 EMPLACEMENT DRIFT
 DEVELOPMENT SEQUENCE

7.2.1 Single Isolation Door Control Constraints

The emplacement drift isolation doors will have multiple functions, including:

- ◆ restricting unauthorized entrance into an emplacement drift loaded with waste packages
- ◆ providing limited shielding from radiation to operations personnel outside the emplacement drifts (for radiation levels outside the doors see Reference 5.6)
- ◆ serving as a ventilation air control device

Each door assembly will consist of a rugged structural steel frame with double leaf type door sections of the side-swing type. The door frame will be firmly anchored to the emplacement drift walls. An alternative to the double leaf door design would be a single leaf door. This single leaf door is presently under design evaluation for use as an emplacement drift isolation door. Since the control requirements are more involved with a double leaf door, this analysis will focus its discussion on the double leaf design. Because there is only one leaf in the single leaf door design, the control requirements for this type of door would be roughly one half those of the double leaf design. The basic material of construction for the doors will be either stainless or carbon steel. The isolation door operating mechanism will be driven by either electric, pneumatic, or hydraulic actuators. The doors will operate from the fully closed position to the fully open position, with no intermediate stops between. The functional and mechanical aspects of the isolation door design are the subject of a separate analysis.

The isolation door at the entrance of each emplacement drift will need to open and close each time entrance into the drift is required. Activities that require entrance into an emplacement drift consist of unloading the emplacement gantry, unloading a WP, removing the gantry, removing WP's, retrieving WP's and unloading/removing the performance confirmation remote inspection vehicle. It is unknown at this time exactly how many times over its life a particular door will be opened and closed, but this number is estimated at over 100. Radiation levels at the emplacement drift entrance will vary depending on how full the drift is with WP's. In any case, these radiation levels may be sufficiently high to warrant remote operation of all isolation doors, taking into account the number of times each of the isolation doors are to be opened and closed.

Sensors and instrumentation can be added to the door assembly to detect whether the door is in the opened or closed position, and this information can be transmitted to a remote monitoring station. A variety of limit switch sensors are available including mechanical-contact, electro-optical and electro-magnetic technologies (Reference 5.7 and 5.13). The specific type of sensor to be used in the design has not yet been determined, however, for illustrative purposes within this analysis a mechanical, push type, spring return limit switches will be used to accomplish this function (Reference 5.9). Limit switches of this type are actuated by means of a rod or plunger located on the top or side of the operating head. Pushing the plunger into the switch assembly causes the contacts to operate. These types of switches can be furnished with adjustable rods minimizing installation and operation concerns. The limit switches can be mounted on support brackets so the door itself contacts the rod which therefore activates the contact in the switch. One switch can be mounted just

inside the drift to monitor the closed door position. Another switch can be mounted such that as the door swings open, the door contacts the switch resulting in a door fully open signal. Refer to Figures 7.2-2 and 7.2-3.

Two switches can be installed on a door leaf, one switch representative of the open position and the other switch representative of the closed position. It is possible for both leaves of the isolation door assembly to be connected by a series of linkages. By monitoring one leaf's position, the position of the other leaf can be implied. This approach is not recommended. What should be monitored is each door leaf's true position. Linkages can jam, disconnect, or break. To say one side of the door is in the same position as the other, which is monitored, leaves a lot to interpretation. Each door's leaf position should be monitored for both the opened and closed position. This approach would require a minimum of four switches per emplacement drift isolation door.

The issue of system redundancy and fault tolerance was not addressed in the previous discussion. The limit switches on the isolation doors can easily be installed in a redundant and fault tolerant configuration. If it is deemed necessary, two relatively inexpensive switches can be installed to monitor each position of each leaf of the isolation door. To monitor the open position one switch can be installed at the top of the door, and one switch can be installed at the bottom of the door. Two switches can also be mounted in the same manner, at the top and bottom, to monitor the closed position of the door. Refer to Figure 7.2-4. This redundant approach would require eight switches per emplacement drift isolation door. Fault tolerance can be achieved by configuring the multiple inputs into redundant PLCs and instituting appropriate software checks similar to those discussed in Section 7.4.1.3. Details regarding the design of the isolation door limit switches can be worked out in the design of the door assembly.

A rotating beacon and alarm horn can be installed at the entrance of each emplacement drift to provide audio and visual alarms for high radiation areas. Prior to the doors actually opening, the alarm horn can sound for a predetermined amount of time. This time can be determined after studying how long it would take a person to safely exit the emplacement drift entrance area, should they happen to be there when the door is directed to open. Whenever the door is open, the rotating beacon can be on to alert personnel who may be approaching that the area should be avoided. Details regarding this portion of the design can be worked out once the radiation levels are more fully understood. The isolation door control system will also be designed with local lock-out capabilities that prevent remote operation of the doors and ensure personnel safety during maintenance or other activities by near the doors.

The emplacement drift isolation door will be furnished with some form of mechanical actuation to open and close it. The door actuator may be electric, pneumatic, or hydraulic. The actuator will require a contact closure to initiate its activation (i.e., solenoid valve, relay). One actuator can be designed, with the addition of linkages, to operate both leaves of the isolation door. Each leaf can also have a separate actuator. If two actuators are used to operate one door assembly, one contact can be used to energize both actuators at the same time, or two separate contacts can be utilized.

FIGURE 7.2-3
ISOLATION DOORS W/ CLOSED
DOOR LIMIT SWITCHES

Based upon the information discussed previously, the inputs and outputs required for the automation of one emplacement drift isolation door can be summarized as follows:

- ◆ Two contact (discrete) inputs for the right leaf open
- ◆ Two contact (discrete) inputs for the left leaf open
- ◆ Two contact (discrete) inputs for the right leaf closed
- ◆ Two contact (discrete) inputs for the left leaf closed
- ◆ One contact (discrete) output for the alarm horn
- ◆ One contact (discrete) output for the alarm beacon
- ◆ Two contact (discrete) outputs for the door actuator(s)

Each door will then require eight discrete inputs and up to four discrete outputs for properly automating the opening and closing operation.

All of the input and output wiring for the operation of an isolation door can be wired from the limit switches, actuators, beacon, and horn to a junction box with individual wires or cables. The junction box could be mounted on the tunnel wall, a short distance from the isolation door. Wiring terminals could be installed within the junction box, where the wiring would terminate. From the junction box a multi-conductor cable could be run to the I/O chassis of the PLC control equipment. This approach should standardize and simplify the component installation and wiring for each door.

7.2.2 Turnover Block Isolation Door Constraints

As stated in section 7.2, there will be a varying amount of emplacement drifts (5 to 22) turned over from the development side of the repository to the emplacement side. It is planned to have a separate network running down both the East main and the West main. Each door can have eight discrete inputs. The turnover block with the most emplacement drifts can therefore have 176 discrete inputs (8 x 22) per main (East and West). Similarly, each door can have four discrete outputs and the largest turnover block can have 88 total discrete inputs (4 x 22) per main. The next step is to take these parameters (176 discrete inputs and 88 discrete outputs per main) and investigate possible alternatives for developing a Programmable Logic Controller (PLC) based control system. The total quantity of I/O for the isolation door network can be obtained by simply multiplying the quantity of doors by these numbers (dependant on repository layout).

Because all of the I/O devices required to effectively monitor and control the isolation door operation will be of the discrete type (on-off), a control system built upon a Programmable Logic Controller (PLC) platform is highly recommended. PLC systems are robust microprocessors specifically designed to process large amounts of discrete I/O such as limit switches, push buttons, indicating lights, horns, and relay outputs (Reference 5.10). These solid state devices employ a programmable electronic memory for storing control instructions to implement specific logic, sequencing, timing, counting, and mathematical calculations. PLCs are programmed using what is known throughout the industry as relay ladder logic (RLL). This programming language is readily understood by most maintenance electricians employed in industrial plants where PLCs are in use. Because of its simplistic structure, RLL is particularly useful in equipment start-up, troubleshooting, and testing situations.

A PLC system can be designed with a remote I/O communication link. The remote I/O link connects remote I/O chassis and other devices to the PLC. The I/O chassis and other devices on the link can be mounted over 3,000 meters from the PLC processor. More than one I/O chassis can be connected to the remote I/O link. A twinaxial cable is simply "series-ed" or looped between the various devices on the link. A remote I/O communication network significantly reduces the amount of field wiring because the I/O racks can be distributed, locating the system I/O terminals closer to the sensors and output actuators.

The repository application lends itself for implementing a PLC system with a remote I/O network because the emplacement side will grow as blocks of emplacement drifts get turned over. A PLC processor and an I/O chassis can be installed in each main of the first turnover block consisting of five drifts. The next turnover block would require only an I/O chassis per main. The third turnover block would also require only an I/O chassis per main. This process could continue until the distance limitation of the I/O network or restrictions of the processor capabilities are reached. At that point another PLC processor and I/O chassis could be installed and the installation sequence can be repeated as the networks extend down the East and West mains.

The above approach allows for the I/O chassis and associated cards of a turnover block, which is ready to be turned over, to be exhaustively checked out prior to connecting to the "real" system. Prior to turning over a block of emplacement drifts, a portable programming terminal can be connected to the I/O chassis to simulate connection to the "on-line" PLC. The door operation can then be started up and the correct operation can be verified. Once deemed satisfactory, the I/O chassis can be connected to the remote I/O link of the "on-line" PLC processor as part of the drift turnover sequence.

The PLC processor for the isolation door control should be furnished with the appropriate number of communication ports to facilitate the remote I/O network and to also communicate to the surface facilities. Communication with the surface facilities can be accomplished with an Ethernet port on the PLC. This port can be connected to the fiber optic backbone which runs in the main and access drifts of the repository. Access to all the points within the PLC database would then be possible from the surface. Commands to open-close a door as well as monitoring the state of all doors could be conducted from the safe confines of the command control center. It is recommended that the PLC processors be provided in a redundant manner so that the secondary PLC can assume immediate control of the system, without interruption to the functionality of the process, in the event of the failure of the primary PLC. A backup control module constantly monitors the self diagnostic features of each PLC. Upon detecting an error bit, the module can switch control from the primary PLC to the backup PLC. If the backup PLC should develop an error, the backup control module can alarm this condition so appropriate maintenance activities can be initiated.

An alternative to a PLC with a remote I/O network would be to install a PLC processor and associated I/O chassis in each turnover block of emplacement drifts. Every turnover block would contain a PLC processor instead of just an I/O chassis with the remote I/O network approach. Each PLC would require an Ethernet communication port to connect to the fiber optic backbone and communicate with the command control center. To avoid single points of failure, all of these PLCs would have to be furnished in a redundant manner. This approach would be more costly than the

remote I/O approach without adding that much more capability or availability. The I/O card structure would be exactly the same. The only difference would be instead of having two, larger, redundant PLCs controlling 63 isolation doors (four turnover panels), there would be eight, smaller, redundant PLCs, each pair controlling the isolation doors in the turnover panel. Also, instead of having two connections to the fiber optic backbone, as in the remote I/O case, there would be eight connections required in the turnover block PLC approach. More hardware also leads to more maintenance and the increased possibility of device failure. For these reasons, redundant PLCs with a remote I/O network is highly recommended.

I/O cards can be replaced with minimal disruption to the process if channel errors are detected on a particular I/O card. Redundancy can also reduce these risks. It is recommended that the PLC processor have two communication ports dedicated to receive/transmit data from/to I/O cards. Each I/O communication port would be connected to a series of I/O chassis or racks. Each chassis would have dedicated I/O cards to process the input or output. The limit switches representative of door position can have one switch wired to a card in one I/O rack and the other redundant switch wired to another card located in the other I/O rack. Refer to Figure 7.2-5. As indicated in Section 1.0, an evaluation of possible failure modes for the PLCs and other equipment will be analyzed in a separate analysis.

The PLC program could be written so that "two out of two" logic will be required to correctly process the information. In other words, both isolation door open inputs must be received by the PLC before the door is recognized as truly open. Inappropriate inputs ("one out of two") can be annunciated so the appropriate maintenance activities can be initiated. The closed circuit television system can be used for an initial assessment of the discrepancies received by the control system.

A PLC system with two remote I/O networks for control and monitoring of the emplacement drift isolation doors is viable. By automating the process, the risk of overexposing personnel is reduced. The system can be designed with total redundancy in mind. Single points of failure can be eliminated from the system design. Redundant limit switches can detect the doors position and reliably transmit the status signals to the PLC system. The PLC system can communicate with the facilities on the surface providing status and control capabilities at the command control center.

7.3 Rail Switch Control System

A rail system will be installed and used to transport the waste packages from surface facilities to the emplacement drifts (Design Input 4.3.5). As stated in section 7.2, there will be a number of drifts turned over at a time from the development side to the emplacement side of the repository. In a manner similar to that of the isolation door control system network, the rail switch control system network should also be designed based on this drift turnover sequence.

The following sections will involve 1) discussing a single rail switch and its operation; and 2) discussing the rail switch control system design and its accommodation of the drift turnover sequence.

7.3.1 Single Rail Switch Control Constraints

A rail switch is a track structure used to divert rolling stock from one track to another. At each emplacement drift turnout there will be a rail switch so the locomotive, WP transporter, and other equipment can exit the main drift and enter the turnout to the emplacement drift entrance. Refer to Figure 7.3-1 for the operation of a rail switch.

Rail switches can be provided with manual, electric, or pneumatic switching devices to activate the rail switch and divert the rolling stock. These switches are very similar in function to the isolation door actuators discussed previously in that they provide the energy necessary to move the rail switch from one position to the other and back. As with the door actuators, a contact output would be required to initiate control action. In addition to the rail switch sensors and actuators, the system may also be required to have traffic lights or rail position indicators that signal the locomotive operators as to the status of each rail switch.

Rail switch circuit controllers act in a manner similar to limit switches in that they provide contacts which change state depending on the switch orientation. The circuit switch controller electrically detects the position of the rail switch. The circuit switch controller can easily be installed in a redundant manner on the rail switch. If it is deemed necessary, two circuit switch controllers can be installed on each rail switch to transmit multiple signals for each position of the rail switch. By adding switch circuit controllers to the rail switch, the correct path of a WP can be determined and modified by personnel in the command control center prior to sending the package underground. Details regarding the design of the circuit switch controllers can be worked out in the design of the rail system. Based upon the information discussed previously, the inputs and outputs required for the automation of one rail switch can be summarized as follows:

- ◆ Two contact (discrete) inputs to the PLC for detecting the switch is "straight- thru"
- ◆ Two contact (discrete) inputs to the PLC for detecting the switch is "diverted"
- ◆ Two contact (discrete) outputs from the PLC for activating-deactivating the switch

Each rail switch will then require four discrete inputs and up to two discrete outputs to/from the control PLC for properly automating its operation.

RAIL SWITCH SET FOR
TRAFFIC STRAIGHT THROUGH

RAIL SWITCH SET TO
DIVERT TRAFFIC

FIGURE 7.3-1
RAIL SWITCH OPERATION

7.3.2 Turnover Block Rail Switch Control Constraints

As stated in section 7.2, there will be blocks or panels of emplacement drifts (5 to 22) at a time turned over from the development side of the repository to the emplacement side. Similar to the isolation door network, there can be a separate network running down each of the mains (East and West). Each rail switch can have four discrete PLC inputs. The turnover block with the most emplacement drifts can therefore have as many as 88 discrete PLC inputs (4 x 22) per main. Similarly, each rail switch can have two discrete PLC outputs and the largest turnover block can have as many as 44 total discrete PLC outputs (2 x 22) per main. The total quantity of I/O for the rail switch control system network can be obtained by simply multiplying the quantity of rail switches by these numbers (dependant on repository layout).

The architecture for the rail switch PLC control system network would be very similar to the isolation door PLC control system architecture for the same reasons presented in section 7.2.2. A PLC system with a remote I/O link is highly recommended for control of the rail switches. A PLC processor and an I/O chassis can be installed in each main of the first turnover block consisting of 5 drifts. The next turnover block would only require an I/O chassis per main. The third turnover block would also require only an I/O chassis per main. Because the I/O for the rail switches is roughly half of that for the isolation doors, the remote I/O link can probably extend farther down the East and West mains before another PLC processor is required. It may be possible that only one redundant set of PLC processors would be required for each main. Details regarding the control system can be worked out as the design progresses.

7.4 Remotely Operated Emplacement Vehicles

The Waste Package Emplacement System concept calls for the use of vehicles that can be manually and/or remotely operated and controlled. The manual and remotely operated vehicles include the primary and secondary Transport Locomotives. The Emplacement Gantry will be strictly remotely operated and controlled. Although the basic requirements, 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, including: similar control system architecture, 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 (the latter is the subject of a separate analysis, Reference 5.11). 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 repository system. It will also help to reduce maintenance and repair costs by standardizing on 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.

7.4.1 Mobile Vehicle Control System Architecture

Control system technologies continue to evolve at a rapid pace. There are many different control architectures that have been developed, but one thing they share is the concept of layers. The functions assigned to the control system are typically distributed across a multi-layered control architecture that includes: the field device layer, the primary control layer, the supervisory control layer, and the operations management or business layer. This section focuses on the on-board device and primary control layers associated with the design of the 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.

7.4.1.1 Background on Vehicle Control Systems

In recent years there has 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 (Reference 5.12, particularly Attachment IV, and Reference 5.13). Mobile, remotely controlled equipment is being used in mining, mass-transit, nuclear, aerospace, defense, manufacturing, plant protection, and plant security industries. The survey found that advanced vehicle control technologies are readily available and could be adapted for use in the repository's unique environment and applications. As indicated in the survey, several vendors have produced ROVs and control components that are designed specifically for nuclear incident monitoring and mitigation (Reference 5.12, Attachment II, and Reference 5.13).

The remote control architectures reviewed in the survey ranged in functionality, complexity, and sophistication from basic PLC technology to systems employing multiple distributed embedded micro controllers, 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 micro controllers 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 micro controllers and MPUs typically provide more programming resources and richer programming environments. Micro controllers 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 multi-tasking capabilities not typically found in PLC technology.

There is precedence within industries such as the automated mining and overhead crane industries, for developing mobile-remote control systems that are based on the relatively simple, well proven, and robust PLC technology (Reference 5.14, 5.15, 5.16). There are also many other examples where safety-critical systems are being controlled reliably by distributed MPU-based architectures (Reference 5.17, 5.18). For the purpose of developing a design concept for viability assessment, the initial 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, for example, 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.

7.4.1.2 Functional Requirements for Emplacement Vehicle Control Systems

The on-board control system concept being developed for the remotely operated emplacement vehicles will be responsible for monitoring and controlling all major vehicle systems, including: 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 the 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 vehicles's performance including: vehicle position, speed, direction, and acceleration; vehicle braking system status; vehicle proximity to other systems, structures and components (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 actuations and instrumentation.

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's 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's control system is designed to be both robust and reliable. As indicated in Section 1.0, 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.

As discussed in previous documents (Reference 5.7, 5.16), the mobile emplacement vehicles will be required to operate in an environment where ambient temperatures may reach 50 °C (Design Input 4.3.4) and radiation levels at the surface of the WPs may reach 37.99 rem/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 colder temperatures.

7.4.1.3 Preliminary Design of the Emplacement Vehicle Control System

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.

For reasons outlined in Section 7.4.1.2 , which include: 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 micro controller or MPU-based systems (See Figure 7.4-1). Later analyses can examine alternative vehicle control systems that are based directly on distributed micro controller 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 power or communication systems, fail-safe brakes would engage and the system would come to a 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. Auxiliary, or backup locomotives could be brought in to continue operations. Other malfunctions would 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. 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 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 7.4-1 Generic Mobile-Remote Control System for Emplacement Vehicles Including the Transport Locomotives and the WP Emplacement Gantry Design Concepts.

As shown in Figure 7.4-1, the initial design of the generic emplacement vehicle control system can be based on a dual-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 the 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 if 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.

7.4.1.4 Vehicle Control Software

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. Developing quality software is vital to system reliability and is a non-trivial element of the design. As with the stationary digital I&C systems, the vehicle control system 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 quality of software that will eventually be developed to control and monitor the 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 and so forth.

Extensive software quality assurance measures are taken in other safety-critical industries that currently rely on digital-based I&C systems. Much can be learned from successful approaches that have been applied in other safety-critical fields such as: aviation, aerospace, public transit, and modern chemical processing and fossil-fuel power plants. It is recommended that a future analysis examine how these other industries have addressed software development, reliability, and testing to achieve successful software-based control systems. It is also recommended that 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.

7.4.2 Emplacement Vehicle Communication Systems

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

Earlier this year, a preliminary analysis of available communication systems was completed (Reference 5.7). Section 7.4.2 of that reference document 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 on 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 all being considered for use in subsurface communication.

Due to the critical need for developing an exceptionally reliable communication system, the current design approach will be to implement dual 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 the use of 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 (Reference 5.17, 5.18).

7.5 Emplacement Gantry System

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 control station. The basic purpose of the Emplacement Gantry is to transport very heavy radioactive waste packages from the emplacement drift dock area, down the length of the emplacement drift, and place the waste packages on pre-installed pedestals. Since, under normal operating conditions, personnel will not be permitted inside the emplacement drifts, 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; physical separation of redundant or backup systems, and others. These design approaches will be utilized where the potential consequences or costs of a system or component failure would be 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 a design analysis entitled: "Evaluation of Waste Package Transport and Emplacement Equipment" (Reference 5.19). The basic mechanical configuration of the Emplacement Gantry is shown in Figure 7.5-1. The purpose of the following sections is to describe the basic control elements of the Emplacement Gantry.

7.5.1 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's mechanical system is presented in Reference 5.19, and a separate analysis also presents preliminary designs for providing power to the mobile emplacement vehicles (Reference 5.11). 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 repository. Initial designs and concepts for the Emplacement Gantry's control and communication systems were discussed previously in Section 7.4. 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 7.5-1, the Emplacement Gantry is designed with four independent DC drive motors, one located at each of the four rocker-bogie wheel assemblies. 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. DC motors will interface directly to motor power and control circuitry housed in on-board electrical cabinets.

FIGURE 7.5-1
EMPLACEMENT GANTRY

There are a wide variety of commercially available variable speed 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's 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 is 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. The braking system 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 a primary consumer of power on-board the Emplacement Gantry. A preliminary analysis of the gantry electrification is provided in Reference 5.11. 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 heat generated by the motors. These cooling systems may be in the form of air conditioning (A/C) units mounted to each of the gantry's electronics enclosures.

There will be several safety factors and design approaches that can essentially eliminate the possibility of derailment. These include: heavy-duty high-quality rails, high quality rail mounts to concrete inverts, slow 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: 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).

WP Lifting Head and Hoisting Mechanisms: The waste package lifting head and hoisting actuators are essential to the successful operation of the Emplacement Gantry. Initial mechanical designs for these actuators are presented in Reference 5.19 and shown in Figure 7.5-1 above. 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 lifting head and 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 DBE's.

The design of the electronic drive controls for the lifting head and hoisting mechanism will employ several factors of 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 waste package. The backup controls and power systems will be diverse, fully redundant, and physically separate systems 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. On the Emplacement Gantry it is envisioned that several separate cameras can be used. 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 waste packages. Special high-radiation cameras are available and can be used (Reference 5.12 and 5.13). 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 near external surfaces of the Emplacement Gantry and will be insulated to prevent radiating heat toward internal components.

Thermal Monitoring and Control Systems: 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 system performance. Equipment operators will be alerted if any temperatures begin to approach predefined operational limits necessitating the gantry to be removed from the emplacement drift. Air temperature can be measured continuously along the emplacement drift during an emplacement cycle.

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 a prior analysis (Reference 5.16). 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) duty cycle of power intensive components, use of low power electronics and components, use of heat tolerant electronics and hardware, and prudent layout of thermal conduction paths for high heat components. Refer to the prior analysis for additional discussion of these design issues and strategies.

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 will continuously monitor the air for minute traces of radionuclide gases, indicating that a waste package has developed a leak. Dosimeters will record cumulative dose radiation exposure to the Emplacement Gantry as a whole. Individual sensors may monitor dose exposures to sensitive electronics mounted internal to the Emplacement Gantry electronic cabinets. These concepts are discussed in more detail in Reference 5.12.

On-board Safety Systems: The Emplacement Gantry will be equipped with a fire detection and suppression system. The fire detection and suppression system will be 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.

Auxiliary Systems and Instrumentation: As indicated earlier (Reference 5.11), the current design concept will utilize an electrified third-rail (conductor bar) system. This concept is reliable, 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 repository conditions. As shown previously in Figure 7.5-1, dual 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 waste packages, 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 encumber 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 monitoring of other chemicals or gases of interest, such as carbon monoxide, or tracer gases if used in the waste package. This capability and related instrumentation are discussed further in a prior analysis (Reference 5.12).

7.5.2 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 7.4 of this analysis presents one of several feasible control architectures, with the gantry based on dual redundant PLC's. The following list is an initial estimate of the I/O interfaces that may be included in such a control system. Note: 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 7.5-1 Emplacement Gantry Vehicle Control 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		

Emplacement Gantry On-Board Systems	AI	AO	DI	DO	SIO	PIO
Actuator Motor Control: Position				2		
Actuator Motor Control: Speed				2		
Limit Switches				16		
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 more exact I/O requirements. Focused analyses on each of the eight gantry systems identified in the I/O list are recommended.

7.5.3 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. Refer to Figure 7.5-2. The Emplacement Gantry Carrier will be driven by one of the Transport Locomotives.

The Emplacement Gantry Carrier will have relatively few, but nevertheless 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 Locomotives' I/O system. 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 series of manually operated latching/restraint mechanisms 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.

FIGURE 7.5-2
EMPLACEMENT GANTRY CARRIER
MECHANICAL ARRANGEMENT

7.5.4 Emplacement Gantry Carrier Control Interfaces

A preliminary estimate of the Emplacement Gantry Carrier electrical interfaces are provided in table 7.5-2 below.

Table 7.5-2 Emplacement Gantry Carrier Electrical Interfaces

Emplacement Gantry Carrier Electrical Interfaces	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 Electrical I/O Totals:	10		8	8	2	2

7.6 Transport Locomotive

The Transport Locomotives will serve as the multi-purpose prime movers of the repository 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, and caretaker activities. During emplacement operations, the Transport Locomotives will be used in tandem to haul waste packages in the Waste 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 Reference 5.19, current concepts for the Transport Locomotives are based on commercially available 45-ton mining locomotives. Power for the locomotives will be provided by a 600 VDC overhead trolley system, and the locomotives will be designed for both direct manual control and wireless remote control (Reference 5.11). The locomotives will be remotely operated when conditions would be unsafe for human operators, for example, all operations near the emplacement drift docking areas. An overview of the current concept of operations can be found in Reference 5.19.

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 Locomotives are shown in Figure 7.6-1. The purpose of the following sections are to describe the basic control elements of the Transport Locomotives.

7.6.1 Transport Locomotive Control Functions

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

Some of these systems are addressed in other, recently completed, analyses. Preliminary designs for the Transport Locomotive's mechanical structure are presented in Reference 5.26, and designs for the overhead trolley power system are presented in Reference 5.11.

FIGURE 7.6-1
TRANSPORT LOCOMOTIVE

A general architecture for the on-board vehicle control and communication systems is presented in Section 7.4 of this analysis. In addition to controlling the operation of the locomotive, the control system for the Transport Locomotives will also 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 Section 7.6.2.

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 7.5.3, while the interfaces between the locomotives and the WP Transport are discussed in Section 7.7.

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. According to Reference 5.27 (pg 1229), many locomotives used in subsurface applications utilize series-wound motors, mounted in a transaxle configuration with a single reduction spur gear transmission. In a series-wound motor the field windings are connected in series with the armature, and therefore, all the current flows through both the field and armature. The motor output torque is directly proportional to two things; the motor input current and the magnetic flux of the motor. Any increases in current also increase 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 Reference 5.27, 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 (or 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 which may otherwise damage the motor. As indicated in previous technology surveys, there is a wide variety of commercial motor controllers available (Reference 5.12 & 5.13).

The current design concept calls for the Transport Locomotives to be equipped with a highly reliable airbrake system typical of those found on most conventional locomotives. Control of the airbrake system is a simple matter of setting and releasing a series of solenoid valves. Federal law requires that locomotives operating in subsurface mining applications have two independent braking systems (Reference 5.27). The control and monitoring of the primary braking system will be performed by the locomotive's on-board PLC. Secondary fail-safe braking systems are typically 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 in order to convert the mechanical energy of a

moving train into electrical energy which is then used to power the locomotive's braking system. This technique is not used to bring the train to a full stop. Further investigation is needed to determine if this technique would be practical and efficient for locomotives used within the 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 7.5. 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 references 5.12 and 5.17, safe and reliable remote control technologies for locomotives have been developed over the last 20 years.

The Transport Locomotives' lighting & camera systems, on-board safety systems, and auxiliary systems will be similar to those described for the Emplacement Gantry in Section 7.5.

7.6.2 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 WHB to the emplacement drift area within the 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 roles 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. Refer to Figure 7.6-2.

There will be electrical and pneumatic interfaces between the primary and secondary locomotives. These interfaces will be effected 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.

FIGURE 7.6-2
ELECTRICAL INTERFACE FOR LOCOMOTIVES
IN TANDEM CONTROL CONFIGURATION

7.6.3 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 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 7.4 of this analysis presents one of several feasible control architectures, and is based on dual redundant PLCs. The following list is an initial estimate of the I/O interfaces that may be included in such a control system. Note: 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 7.6-1 Transport Locomotive Control: 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					

Transport Locomotive On-Board Systems	AI	AO	DI	DO	SIO	PIO
IV. Tandem Locomotive Control Interface						1
V. Locomotive Interface with WP 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 indicate 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.

7.7 Waste Package Transporter

The Waste Package (WP) Transporter is a massive, highly shielded, completely enclosed rail car that will be used to transport the radioactive waste packages from the Waste Handling Building at the surface, down into the emplacement drift area of the repository. The WP 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 WP Transporter was recently the subject of a separate analysis (Reference 5.26). The basic mechanical layout can be seen in Figure 7.7-1. In its current design configuration, the shielding used to form the walls, floor, crown and doors of the WP 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 WP Transporter will be equipped with its own set of air brakes and a redundant backup set of spring-loaded fail-safe brakes. The WP Transporter will have a set of double doors at one end. These doors will be opened and closed by two heavy duty gear motors mounted in-line with the axis of the door hinges.

Inside the WP Transporter will be a WP loading and unloading mechanism. The loading mechanism will consist of two main systems; a rail-based shuttle car (also known as the "reusable rail car"), 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 WP Transporter will be a camera system for remote viewing, along with radiation and thermal monitoring instrumentation.

The operation and functions of the WP Transporter will be remotely controlled. Control commands will originate either from the operator located on the primary locomotive, or they will originate 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 transferred to a PLC-based control system located on the WP Transporter. The PLC on the primary locomotive will monitor and check all operations and system performance parameters of the WP Transporter.

The overall reliability of WP 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.

FIGURE 7.7-1
WASTE PACKAGE TRANSPORTER

When empty, the WP Transporter will be fully accessible inside and out by personnel for routine and preventative maintenance. Because the WP Transporter's 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.

7.7.1 Preliminary Waste Package Transporter Input/Output List

The WP 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 WP Transporter 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. Table 7.7-1 is an initial estimate of the I/O interfaces that may be included in such a control system. Note: 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 7.7-1 Waste Package Transporter: Input/Output List

WP Transporter On-Board Systems	AI	AO	DI	DO	SIO	PIO
I. WP 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					

WP Transporter On-Board Systems	AI	AO	DI	DO	SIO	PIO
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. WP 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 WP Transporter						1
Preliminary Estimate of WP Transporter Control System I/O Totals:	46	4	18	31	6	5

The preliminary estimate of control system I/O totals for the WP Transporter indicate 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.

7.8 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 YMP RAM plan (Reference 5.20). 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 begin to identify and outline RAM issues.

A RAM analysis of the emplacement system will assess the availability for various design concepts as the design evolves. Expressions for availability will be based on the System Description Document (SDD) requirements and coordinated with a simulation code throughput modeling effort. The modeling effort will use the guidelines provided in appropriate references such as 5.21 and 5.22.

Quantitative system availability analyses are performed to determine if the SDD availability requirements are met.

Designing for adequate availability will involve provisions for redundancy in subsystems and/or hardening to withstand the environment where deemed necessary, depending on the criticality of a given operational function without interruption during the mission time. A highly critical function, for example, is the ability to move the gantry while carrying a WP in the emplacement drift without a breakdown of the drive motors or associated control systems because maintainability (corrective maintenance) is more difficult in the emplacement drift. By 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.

In addition, the possibility of failures induced by human error needs to be addressed for their 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.

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 the radiation and thermal hazards. Corrective maintenance of the subsystems on the locomotives and WP transporter can also most likely 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 (R&R) maintenance philosophy. The design would accommodate ease of access and connectors and fasteners to facilitate R&R. 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 (RCM) will be applied to

assure a suitably low probability of failure during the mission time. Nevertheless, 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 and temperature in the emplacement drifts and somewhat elevated temperatures in the turnouts which 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.

7.8.1 RAM Issues Related to the Emplacement System

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 waste packages it will be inaccessible to personnel. It is very important that the remote emplacement system works reliably. The consequences of a failed emplacement gantry inside an emplacement drift can be significant. Conversely, the instrumentation installed in the perimeter mains for control of the isolation doors and rail switches, on the locomotives, and on the WP transporter will be accessible to personnel for periodic testing, calibration, and repair or replacement and do not appear as significant RAM concerns. Therefore, this section provides an initial discussion focused on RAM issues related to the emplacement system required to operate within the emplacement drift.

The principal subsystems of the mobile remote emplacement system pose different RAM issues, depending on their function and criticality to mission success, as follows:

Locomotive 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, 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. RCM should be applied to determine the optimal test and/or refurbishment program for the control system.

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, driving 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. RCM should be applied to determine the optimal test and/or refurbishment program for the control system.

Communication System - Failure of the communication system is similar to that of the control system. Portions of the communication system 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 and 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 (R&R) 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 (e.g., R&R) can be performed quite readily by driving the gantry back 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.

7.8.2 Recommendations for a Future RAM Program

The future RAM analysis program for the emplacement system will 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 of 100 years. 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

- Applications of Preventive Maintenance (PM) and Reliability-Centered Maintenance (RCM) concepts
- Human Reliability Analysis (HRA) during operations and maintenance, installation, configuring for specific mission
- 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 Design Basis Events (DBEs)

Reference 5.21 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 methodology for RAM analysis and design support. Although Reference 5.21 was developed at a time when salt-dome sites were being considered, the techniques for defining, prioritizing, and analyzing RAM elements remain relevant. Techniques for simulation modeling are not included in Reference 5.21 since they had not been developed at that time.

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; Maintainability Checklist)
- Failure Mode and Effects Analysis (FMEA) [or a variant such as Failure Modes, Effects and Criticality Analysis (FMECA)]
- Reliability Block Diagrams (RBD)
- Maintainability Evaluation (e.g., estimates of access times, repair times, radiation exposure of workers, etc.)
- Fault Tree Analysis (FTA); for detailed reliability analysis of subsystems and systems)
- Event Tree Analysis (ETA); 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 FMEA, RBD, FTA, and ETA provides a structured technique to examine how and why a mission may fail or why a failure may be critical. The quantitative application of these techniques can help in optimization of cost vs performance. If deemed appropriate, the operation of the emplacement system can be modeled in a simulation.

To support a quantitative analysis, including simulation, the RAM program must also include a database development. 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.

7.9 Repository Supervisory Control and Data Acquisition (SCADA) Network

This section presents an overview of the repository Supervisory Control and Data Acquisition (SCADA) network for the emplacement system. It will discuss how the data may be handled, presented, stored and displayed to the operator. An initial estimate of the total system Input/Output (I/O) requirements will also be discussed.

7.9.1 Network Overview

A network can be defined as a collection of communicating devices that are interconnected and autonomous (Reference 5.23). All of the following conditions are essential for a functional network:

- ◆ A communicating device is any system that transmits or receives data. A communicating device can be a mainframe, personal computer, modem, controller board, or telephone.
- ◆ The interconnection of devices asserts that this equipment can exchange data. The interconnection may be over some physical medium, such as optical fiber, or through the air via radio waves or laser optical systems.
- ◆ The devices on the network are autonomous, or "crash independent". That is, failure of a single device does not cause other devices to become inoperable and bring down the entire network.

The repository network equipment required for the remote emplacement operations will incorporate the features described above. Monitoring and control systems such as PLCs, radio frequency (RF) modems, and video transmission equipment will all be interconnected via the fiber optic backbone that runs throughout the subsurface main drifts. The particular topology of the network requires further investigation and design effort. Brief discussions of the various topologies follow.

In a star topology (Reference 5.23, 5.24), all devices on the network are interconnected through a central node. All communication is from one device to another with the central node acting only as a switch to provide a pathway between pairs of devices attached to it. A good example of a star network is a telephone switchboard, since access from one station on the network can occur only through the central device. The central node does pose high single point of failure concerns. This topology does not appear to be well suited for the repository application.

In a bus topology (Reference 5.23, 5.24), a cable is usually laid out as one long branch onto which smaller branches are used to interconnect each station to the main data highway. Bus networks can be compared to the way appliances in the home are connected to the AC power line. Buses are probably one of the oldest network topologies. Buses are usually limited in the communicating medium that they can use, but do not typically suffer from single point failure problems.

In a ring topology, the communicating devices are connected by a set of point-to-point links that are organized in a closed fashion. Rings are commonly employed in networks. If one link of the ring is cut or disconnected, the entire network remains on-line. This is because the communications are

bi-directional within the circular ring. The communications software can even locate the point where the disconnection or break has occurred.

Some networks are a mixture of topologies. Because of the inherent reliability and reduced single failure potential of a heterogeneous topology, the repository network design will incorporate this approach. A redundant ring can be installed around the perimeter of the repository such as down the North ramp, then down the West main, and eventually back out the South ramp to the surface facilities. Off of this redundant ring can be other smaller redundant rings such as down the exhaust main and the East main. This approach would require that the cable be routed on the surface between the South Portal and the command control center located near the North Portal. Refer to figure 7.9-1 for a depiction of the interconnection of the repository SCADA devices. The entire aspect for the proper network to be installed in the repository requires additional design effort and investigation.

7.9.2 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 view and manage this information. It is anticipated that the emplacement system command control center will consist of a control room from which all subsurface emplacement operations can be monitored and controlled. This control room will be equipped with engineering workstations, mainframes, control consoles and graphics terminals that can provide the operators with direct real-time data. Sufficient storage capacity should exist for time-stamping the data as it is received.

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 underground and have access to the transmitted data and assume control of emplacement equipment. Versatility, accuracy, timeliness, and robustness are all attributes that can be implemented in the emplacement process control system.

7.9.3 Estimated Size and Complexity

From the information stated previously, there can be approximately 2,500 points from the isolation door control system, approximately 1,300 points from the rail switch control system, approximately 650 points from the emplacement gantry control system, and approximately 250 points from the locomotive control system (including WP transporter and gantry carrier signals). Allowing a design contingency of 1300 points puts the total number of points for the emplacement system at 6,000 points. There will also be between six and ten video signals from the emplacement gantry and emplacement locomotive requiring digital signal transmission to the surface facilities. Therefore, both data and video signals will be required to be transmitted over the fiber optic backbone to facilitate the emplacement process. The fiber optic backbone which may be installed in the repository could operate up to and in excess of 150 million bits/sec (Mbps). (Reference 5.23) However, the software must be configured to handle this high data rate. To be conservative, it can be assumed that the network can handle a data rate of 100 Mbps.

FIGURE 7.9-1
SCHEMATIC BLOCK DIAGRAM
REPOSITORY SCADA NETWORK

Compressed digital video data transmission rates are completely variable from 1.5 to 8.5 Mbps. Utilizing different rates one can match the video quality to the complexity of the video being transmitted. Data rates can be increased to produce higher quality for complex, fast-motion pictures, while lower data rates can be applied to transmit more simple, slow moving video to conserve on available bandwidth. The commonly referred to international standard for digital video compression is called Moving Pictures Expert Group (MPEG)(Reference 5.25). MPEG-1 is designed for delivering video from a CD-ROM. MPEG-2 is specifically targeted at digital transmission and supports a much wider range of resolutions and bit rates than MPEG-1. The repository application would follow the MPEG-2 standard. For example, with ten video signals from the emplacement system, with an average of 5 Mbps each, then 50 Mbps of the network transmission capability will be needed to support video transmission.

Analog values are usually converted to digital signals in 12 or 16 bit resolution. If the remaining data rate of the network (50 Mbps) is divided by 120 bits, which could be representative of one analog value with start delimiter, addressing, and end delimiters, the network can support transmitting over 400,000 analog values every second. Performance confirmation has roughly 35,000 points (Reference 5.16), the emplacement system could have 6,000 points, and repository operations (utilities such as ventilation control, radiation monitoring, environmental monitoring, etc.) will have numerous points, but the total will undoubtedly be less than 400,000. It is therefore highly doubtful that the network will become saturated and data becomes lost or not updated in a timely manner. Faster network speeds will only increase the number of points available for transmission.

For the underground repository it is recommended that a broadband transmission system be implemented. Channels can be assigned to communicate between dedicated pieces of equipment. A number of channels can be assigned to strictly transmit data to and from the isolation door control systems and rail switch control systems. Some channels can be assigned to transmit video signals and data streams to and from the emplacement gantry, while other channels can be assigned to transmit video signals and data streams to and from the transport locomotive and waste package transporter. With the deployment of a Broadband Integrated Service Digital Network (B-ISDN), it will be possible to have a network capable of supporting both the low speed and very high speed that these services require. In the past, video, audio, voice and data services needed different types of communication channels. One of the main advantages of B-ISDN is the ability to integrate these features over the same network and cable. This will allow the operators of the repository immediate access to the data and video items of interest.

8. CONCLUSIONS

This analysis met its objectives by performing the following activities. This analysis identified and discussed various methods for monitoring and controlling the operation of the stationary equipment such as the isolation doors and rail switches (see Section 7.2 and 7.3). Methods for monitoring and controlling the operation of the mobile equipment such as the emplacement gantry, emplacement locomotives, WP transporter, and gantry carrier were also identified and discussed in sections 7.4, 7.5, 7.6 and 7.7. Due to the unqualified/unconfirmed input data used in the preparation of this analysis, the output/conclusions from this analysis can not be used as input into documents supporting procurement, fabrication, or construction unless they are controlled and tracked as TBV or TBD in accordance with NLP-3-15 or other appropriate procedures.

Section 7.1 identified several issues related use of digital control and instrumentation within regulated nuclear environments. Four of these issues are addressed, at least initially, within the scope of this analysis. It is recommended that the other four issues including: safety and reliability assessment methods, human factors and human-machine interfaces, the current case-by-case NRC licensing process for digital I&C systems, and adequacy of the NRC's technical infrastructure, be investigated and addressed in future analyses.

As a result of the discussions in section 7.2 and section 7.3, it is recommended that the stationary equipment such as the isolation doors and rail switches each have their own independent network of PLCs for localized control. The PLCs should be provided in a redundant configuration so that there can be no single point which can result in system failure. The PLCs should have the capability to communicate with the main repository control system, which provides the integrated services necessary for the emplacement process. PLCs in general are robust, environmentally hardened machines which can operate in ambient temperatures up to 60 °C (Reference 5.10). Preliminary estimates of the I/O required for automating the operation of these devices were included in their respective sections.

The PLCs that control the stationary equipment should communicate with the main repository control system via a redundant fiber optic backbone which will run in all main and access drifts, not in the emplacement drifts. The fiber optic backbone, as discussed in section 7.9, should be a broadband based transmission system which can be subdivided by various frequencies to form subchannels, with each subchannel permitting transfer of data and video signals independently of data and video signals on another subchannel.

Section 7.4 presented a viable design of a vehicle control system that can be used as the basis for both the Emplacement Gantry and the Transport Locomotives. The control system can be based on a dual redundant PLC control concept support by auxiliary on-board microprocessors. The control system can be robust and reliable, and 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 many sources. A brief discussion of the vehicle control software and mobile communication systems were also discussed. Other control architectures, based on distributed microprocessor or micro controller systems, are also possible and should be examined in later analyses.

Future design work will also need to adequately address the significant quantity of software that will eventually be developed to control and monitor the repository. 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 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.

Section 7.5 described 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 lifting head and hoist mechanisms, vision systems, thermal monitoring and control, radiological monitoring systems, and on-board safety systems. Section 7.6 described similar design concepts for the Transport Locomotives. Also discussed in Section 7.6 were the control interfaces between the Transport Locomotives and the WP Transporter and Emplacement Gantry Carrier.

In addition to the initial design of these key systems, information was presented relating to the issues of equipment reliability, availability, and maintainability (RAM). Recommendations for a future RAM analysis and program have been discussed in section 7.8.

Automation of the emplacement process appears to be very viable. The technology exists for remotely operating all of the equipment involved in the transport and emplacement of the waste packages. By implementing remote control, worker safety should be enhanced by eliminating exposure to harmful radiation. Another reason to implement remote control is to effectively eliminate the human error factor. Even though human operators will oversee the emplacement operation, software and hardware interlocks will be incorporated in the design so that all the equipment operates in a safe and reliable manner.

9. ATTACHMENTS

Not used.