RFP DOT-2040 Section VI.D

State of California
Department of Transportation
District 11

I-15 Reversible Lane Control System (I-15 RLCS)
Application Software Requirements Specification

***** to be finalized by contractor *****

April 21, 2004

Modification History

After the baseline version of this document is approved, any changes made to the document must be approved in accordance with the provisions of the established Change Management Plan.

Table of Contents

1. Introduction

1.1. Purpose

This document defines the application software requirements for the Interstate -15 Reversible Lane Control System (I-15 RLCS).

The RLCS application software ('RLCS Application') will meet all of the software requirements listed in this document, and if any changes are made to the original set of requirements, this document will reflect those changes upon approval of project management and the appropriate stakeholders.

1.2. Scope

The purpose of the (I-15 RLCS) is to open and close the reversible lanes for morning and evening peak traffic hours and any special events defined by operators of the system. The software developed from this specification will replace the current aging and non-expandable RLCS Application. In addition, new controller devices, as well as field device interface cards will be provided by the successful bidder, and the software will interface with these new field hardware components via interfaces to driver software.

1.2.1. Objectives

The RLCS Application must support the objectives listed in Section 1.2 System Goals, in the System Requirements Specification.

1.3. Definitions, acronyms, and abbreviations

See Appendix B for a list of terms used in this document.

1.4. References

The reference documents below were used to prepare this requirements document:

Title	Prepared By	Date
I-15 Reversible Lane Control System Existing Systems Documentation Report	Caltrans	June, 1998
I-15 Reversible Lane Control System System Requirements Document – Version D	Caltrans	March, 2002
I-15 Reversible Lane Control System Project – User Requirements Document – Version D	Caltrans	December, 1998
I-15 Reversible Lane Control System Feasibility Study Report	VIP	July, 2001
IEEE Recommended Practice for Software Requirements Specifications 830-1998	IEEE	1998
IEEE /EIA 12207.1 – 1997: Guide for Information Technology Software Life Cycle Processes – Life Cycle Data	IEEE SESC (Software Engineering Standards Committee)	1997

Exhibit 1.1 - Reference Documents

Appendix A provides a Traceability Matrix that maps the System Requirements to this document.

1.5. Overview

The remainder of this document is divided into two sections.

Section 2 gives a high-level, user- and operationally-oriented view of the software.

Section 3 provides the detailed requirements including explicitly stated and derived functional requirements from which the RLCS Application will be designed.

2. Overall description

This section describes the general factors that affect the RLCS Application software requirements. This section does not state specific requirements, instead it provides a background for those requirements, which are defined in detail in Section 3.

The RLCS Application will allow an operator to view system status and issue commands to change device status as well as configure the system and generate reports. The five major functions of the RLCS application software are a Graphical User Interface (GUI), Process Control and Monitoring, Sequencing, Data Processing and Security, and Reporting.

2.1. Product perspective

This section describes how the RLCS Application software relates to other systems and software as well as how it functions internally.

2.1.1. External System Interfaces

2.1.1.1. In addition to providing data to the system users and traffic operations management, the RLCS Application will provide data to other external systems via an external server data store accessible by other external systems such as ATMS-2, ValuePricing/FasTrak, and ATIS.

2.1.1.2. The RLCS Application will also allow for remote access through a firewall via outside telecommunications networks by authorized users.

The diagram below shows the flow of information to and from the different interfaces.

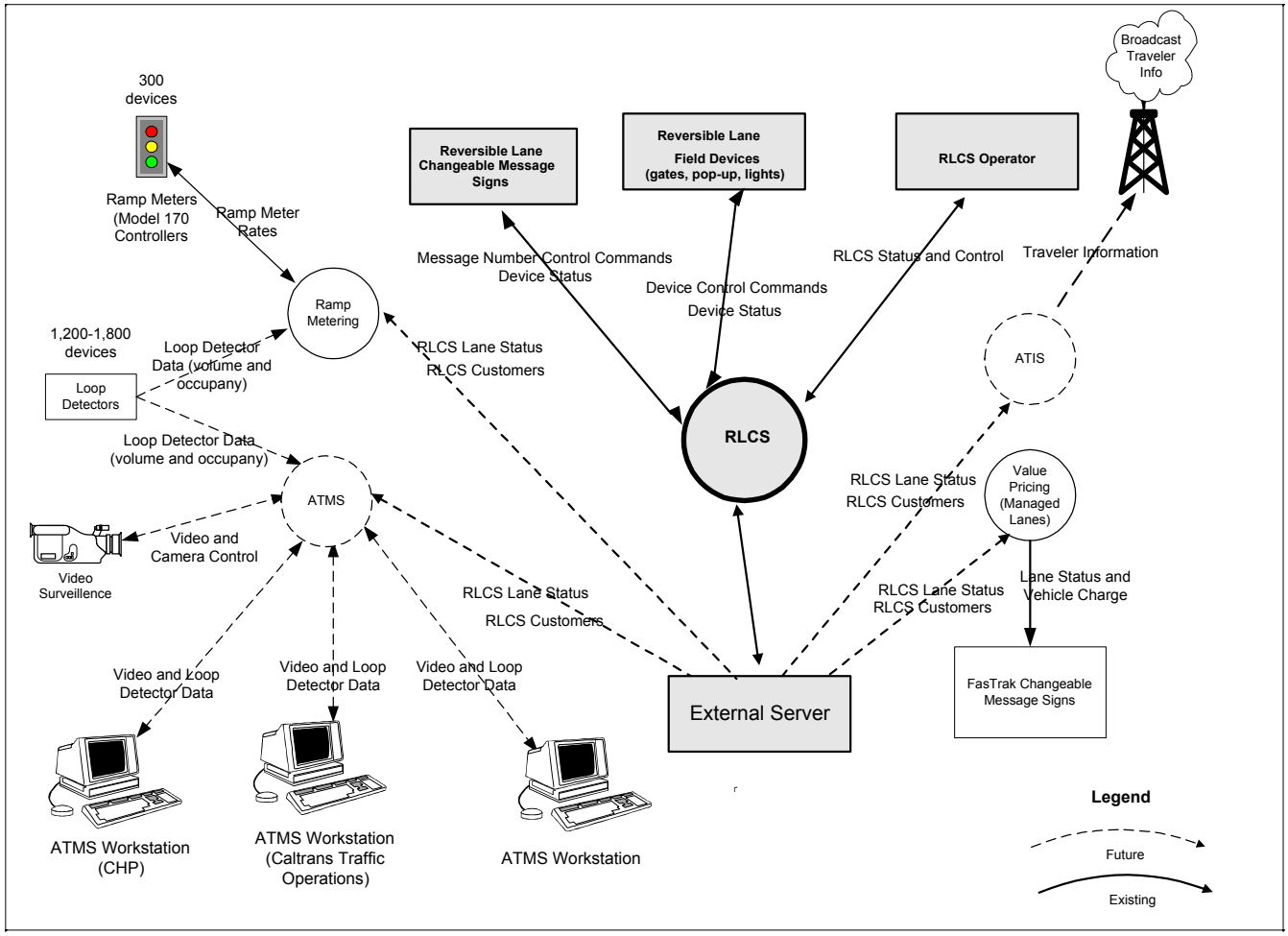


Exhibit 2.3: External RLCS Application Interfaces

2.1.2. User Interface

The user will operate the RLCS Application software using a graphical user interface.

2.1.3. Hardware Interfaces

RLCS application will seamlessly interface and control hardware devices.

2.1.4. Software Interfaces

This section discusses interfaces between the RLCS application and other software, which may include but are not limited to: Workstation O/S, Network O/S, Controller O/S, a database management system, and a reporting tool

2.1.5. Communications Interfaces

The RLCS will provide access to system status data, to external systems through a firewall. This will be a one way data transfer to a computer outside of the RLCS network and making it available there for public use. The transfer will occur every 30 seconds. A one way serial data transfer will also be provided.

RLCS workstations and controllers will reside on a private network to communicate field device information.

The RLCS private network communication media will include fiber, Cat 5 wiring Leased lines and dial-up lines

Communications from the TMC to the DCU controllers is through the FCU controller. In addition, wireless connections between the FCU and DCU controllers are not an option due to security and interference considerations

2.1.6. Memory constraints

The only memory constraints imposed on the software will depend on constraints associated with the intelligent controller selected for the system. For the 2070 controller, reference the TEES document in Appendix E.

2.1.7. Operations

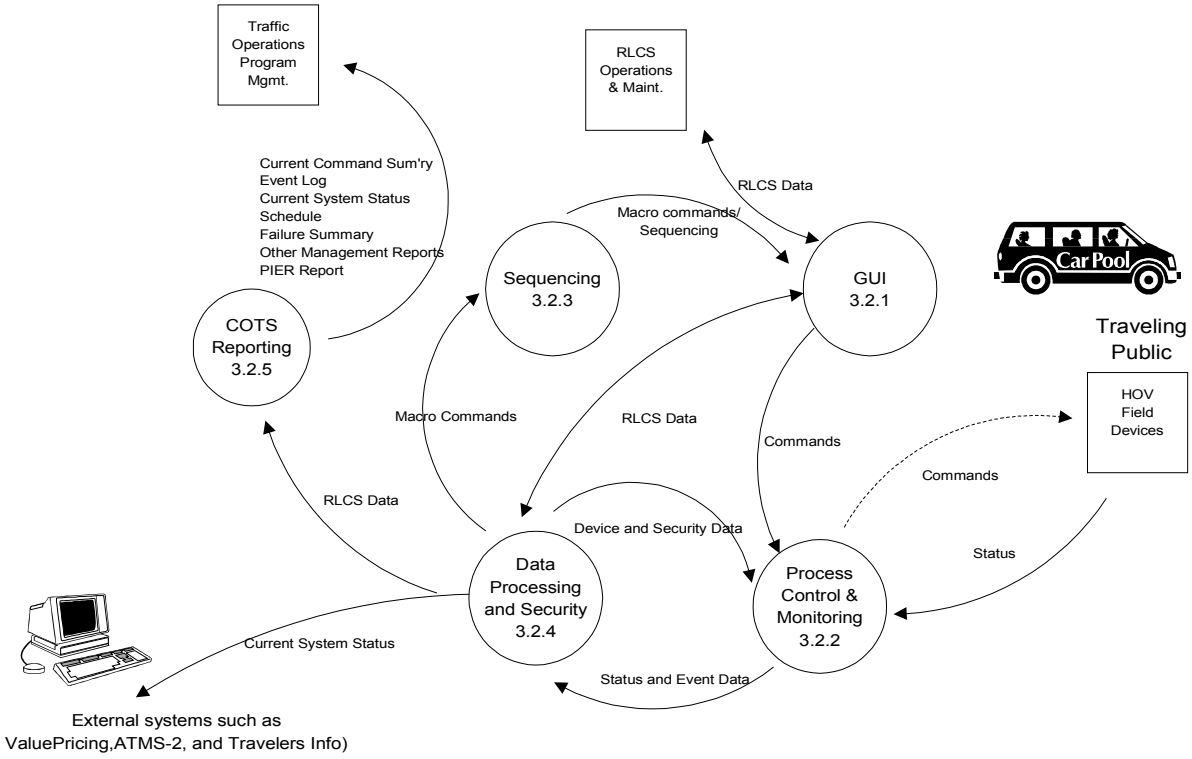
The RLCS Application will support the operations described in ‘Section 2.8 Operational Scenarios’ of the RLCS System Requirements Specification..

2.1.8. Site Adaptation

The RLCS Application will operate as a component of the RLCS System, for which physical adaptations are described in ‘Section 3.7 Physical’ of the System Requirements Specification

2.2. Product functions

The data flow diagram below shows the five major functions of the RCLCS Application : GUI, Process Control and Monitoring, Sequencing, Data Processing and Security, and Reporting.



I-15 Reversible Lane Control System
Level 1 - Data Flow

Exhibit 2.5: I-15 RLCS Product Functions Data Flow

2.3. User characteristics

Several classes of users will access the RLCS Application. A user is defined as anyone who has the ability to 'log on' to the RLCS. External entities such as ATMS and ValuePricing, which will retrieve data from a server external to the RLCS network, are not considered users. Also, the driving public will have access to system status via the changeable message signs, and eventually the Traveler Information Network, but are also not considered users of the system.

User Class	Functions
Operator	Command control of the system during normal mode. Only one 'operator' may be logged onto the system at any given time. Authorized to change system mode.
Management	Reporting and status checking capabilities only
Field Maintenance Staff	Command control of the system only during maintenance mode. Ability to execute maintenance mode control sequences from FCU workstations or remote dial-in terminals, as well as from the maintenance building workstation, but not from the TMC workstation. Not able to change system mode.
Electrical Systems (Hardware)	Reporting and status checking.
Software Systems (Software)	Reporting and status checking.
System Administrator	A member of the District 11 technical staff (usually a Software Systems staff member) authorized to create and modify system configuration data, including staff, devices, and scheduled operations. Authorized to changed system mode.

Security setup capabilities are defined in more detail in Section 3.

2.4. Constraints

The following constraints were factors in the development of the detailed requirements for the RLCS Application:

a) Regulatory policies – There were no technical regulatory policies specifically covering the RLCS Application.

b) Hardware limitations – The RLCS Application will reside on a hardware platform compatible with Microsoft Windows NT or Unix-based operating systems.

c) Interfaces to other applications – Other than system level interfaces, such as network, operating system, and database system, there will be no interfaces to other applications.

d) Parallel operation – For a short time, while the RLCS Application is being deployed in the field, the existing system will be left in place and will only be disconnected after a successful, complete system test in the field during hours when the facility is closed to traffic.

e) Audit functions – The RLCS Application will create and store log files which will track all

application activity.

f) Higher-order language requirements – There are no specific high level language requirements, other than that a high level language be used to develop and maintain the RLCS Application for more cost-effective maintenance efforts.

g) Reliability requirements – The RLCS Application must be available 24 hours per day, 7 days per week, 365 days per year.

h) Criticality of the application – The RLCS Application is important to the traffic management goals of the Southern California region. Opening the lanes in the direction of the peak traffic flow to route traffic onto the reversible lanes is a critical operation in meeting these goals.

i) Safety and security considerations – The safety of field maintenance staff and the traveling public is dependent on the correct functioning of the RLCS Application to open and close the facility.

Reversible Lanes facilities, whether operated manually, or by a control system, present a fundamental risk: The risk is the possibility of opening an entrance for one direction of travel, with one or more entrances already open in the opposite direction.

Should this type of event actually occur, it would be nothing less than catastrophic; for the motorists involved; for the traveling public in general, for the system operators, and for the Agency.

Another potential control system risk, lies with the barrier gates used at Locations 1, 2, and 5. Should one of these gates be lowered across an otherwise open entrance, the results could be catastrophic.

There are less serious, but possibly more common control system risks in closure device/sensor failures during the opening or closing of an entrance.

In the absence of full system overrides, if the system allows, or causes, an entrance to be opened in one direction, when an entrance in the opposite direction is open, then the system has failed.

A well designed, carefully implemented, and thoroughly tested control system, can reduce the chance of such an occurrence (due to operator error, control system or sensor failure).

In order to achieve this, the nature of the risk must be understood and continually kept in mind by control system developers and testers.

2.5. Assumptions and dependencies

The RLCS will benefit from the deployment of the Fiber Optic Network along I-15 Reversible Lane corridor to include the RLCS lanes. The communications between the FCU and DCU locations will continue to be copper. The primary mode of communication is fiber and secondary is ISDN. The fail over will be transparent to the RLCS application.

.

A dialup connection will be used for remote access to the RLCS.

2.6. Apportioning of the requirements

The RLCS software will not be apportioned, or split between multiple releases. The complete set of requirements will be included in one release.

3. Specific Requirements

This section of the SRS contains the RLCS Application software requirements to a level of detail sufficient to enable designers to design the system, and acceptance testers to test that the system satisfies the requirements.

These software requirements will be revised by the contractor to reflect the final approved RLCS architecture design. This will be done before high-level software design phase.

Every stated requirement is externally perceivable by users, operators, or other external systems.

This section describes each input into the software, every output from the software, and all functions performed by the software.

3.1. External Interface requirements

3.1.1. Hardware Interfaces

Multiple field devices will interface with updated device input/output cards that in turn will interface with an intelligent controller. It is unknown at this time which particular controller will be used to control the field devices, but the software must interface with whichever controller is chosen to interface with the field devices. The field devices and controllers in the table on the following page are currently in use at the facility. See Appendix D for a table of current FCU-DCU and FCU-CMS interface pin configurations.

3.1.1.1 Field Device I/O Drivers

The RLCS software shall send to and receive data from the field device I/O cards through I/O driver software.

The tables below show the description and locations of the field devices currently installed and to be installed at the facility. Appendix D contains a chart with I/O card pin configurations.

Field Device	Description	FCU-S*			FCU-N*		Comments
		DCU 1	DCU 2	DCU 3	DCU 4	DCU 5	
MCU	Manual Control Unit	1	1	1	1	1	Type of devices Controlled by each FCU controller.
Gate	Barrier Gate	1	1	0	0	1	
Draw Lights	Entrance Street Lights	1	1	0	0	1	
Wrong Way Lights	Barrier Lights	1	0	1	1	0	
EL-1	Longitudinal Entrance Pop-Up	3	2			5	Number of pop-ups per bank.
EL-2	Longitudinal Entrance Pop-Up	5	5			6	
EL-3	Longitudinal Entrance Pop-Up	4	9			6	
EL-4	Longitudinal Entrance Pop-Up	5				6	
EL-5	Longitudinal Entrance Pop-Up	6				3	
ET-1	Transverse Entrance Pop-Up	7	9			8	
WL-1	Longitudinal Wrong Way Pop-Up	4		4	4		
WL-2	Longitudinal Wrong Way Pop-Up	5		5	7		
WL-3	Longitudinal Wrong Way Pop-Up	5		7			
WL-4	Longitudinal Wrong Way Pop-Up	4		7			
WL-5	Longitudinal Wrong Way Pop-Up			7			
WT-1	Transverse Wrong Way Pop-Up			5	10		
WT-2	Transverse Wrong Way Pop-Up	6			11		
CMS 1-4	I-15 northbound RLCS approach						Controlled from FCU South
CMS 5-8	SR 163 northbound RLCS approach						Controlled from FCU South
CMS 9-12	I-15 southbound RLCS approach						Controlled from FCU North

Exhibit 3.1: I-15 RLCS Controllers and Field Devices

*The controllers at the FCU and DCU will be replaced with modern controllers such as the Department of Transportation 2070 Advanced Transportation Controller (ATC) or a controller with equal or better capabilities.

RLCS Inputs to and outputs from the FCU and DCU Controllers

Field Device	*Device Sensors*	*Inputs Or Outputs*	*FCUS*	*FCU-N*	*DCU 1*	*MCU 1*	*DCU 2*	*MCU 2*	*DCU 3*	*MCU 3*	*DCU 4*	*MCU 4*	*DCU 5*	*MCU 5*	*Total # of Sensors*
Barrier Lights	LHS and LHN Light	Output	4	4	1	0	1	0	1	0	1	0	1	0	13
FCUs and DCUs	Cabinet ID	Input	4	4	0	0	0	0	0	0	0	0	0	0	8
	Compressor Pressure	Input	1	1	0	0	0	0	0	0	0	0	0		2
MCU	Air Tank Press	Input	1	1	0	1	0	1	0	1	0	1	0	1	7
	Line Air Press	Input	0	0	0	1	0	1	0	1	0	1	0	1	5
	Auto/ Manual	Input	0	0	0	1	0	1	0	1	0	1	0	1	5
Pop-Ups	Pop-Up Power Enable	Output	0	0	1	0	1	0	1	0	1	0	1	0	5
	Pop-Up Entrance Up	Output	0	0	6	0	4	0	0	0	0	0	6	0	16
	Pop-Up Entrance Down	Output	0	0	6	0	4	0	0	0	0	0	6	0	16
	Pop-Up Wrong Way Up	Output	0	0	5	0	0	0	6	0	4	0	0	0	15
	Pop-Up Wrong Way Down	Output	0	0	5	0	0	0	6	0	4	0	0	0	15
CMS	CMS	Input/Output	8	4	0	0	0	0	0	0	0	0	0	0	12
Gate	Gate Power Enable	Output	0	0	1	0	1	0	1	0	0	0	1	0	4
	Gate Warning Lights	Output	0	0	1	0	1	0	1	0	0	0	1	0	4
	Gate Up	Input/Output	0	0	1	0	1	0	1	0	0	0	1	0	4
	Gate 15 Deg. Down	Input/Output	0	0	1	0	1	0	1	0	0	0	1	0	4
	Gate Down	Input/Output	0	0	1	0	1	0	1	0	0	0	1	0	4
	TOTAL # OF SENSORS:		18	14	29	3	15	3	19	3	10	3	19	3	139

Exhibit 3.2a: Currently installed I-15 RLCS Field Sensors and Devices

Devices to be added to the RLCS are shown in Exhibit 3.2b.

RLCS Inputs to and outputs from the FCU and DCU Controllers

Field Device	*Device Sensors*	*Inputs Or Outputs*	*FCU-S*	*FCU-N*	*DCU 1*	*DCU 2*	*DCU 3*	*DCU 4*	*DCU 5*	*Total # of Sensors*
FCUs	Watchdog Timer	Output	1	1	0	0	0	0	0	2
FCUs/DCUs	Watchdog Status	Output	1	1	1	1	1	1	1	7
	Temp	Input	1	1	1	1	1	1	1	7
	Voltage	Input	1	1	1	1	1	1	1	7
FCUs	Yard Gate Sensor	Input	1	2	0	0	0	0	0	3
	Equipment Room Sensor	Input	1	1	0	0	0	0	0	2
	Control Sensor	Input	1	1	0	0	0	0	0	2
	Fire Alarm	Input	1	1	0	0	0	0	0	2
	Back-up AC Power Sensor	Input	1	1	0	0	0	0	0	2
	AC Power Monitor	Input	1	1	0	0	0	0	0	2
	Reset I/P Jack	Input	1	1	0	0	0	0	0	2
	Air Dryer Sensor	Input	1	1	0	0	0	0	0	2
	Air Cooler Sensor	Input	1	1	0	0	0	0	0	2
	Air Compressor Monitor	Input	1	1	0	0	0	0	0	2
	Air Compressor Power	Input	1	1	0	0	0	0	0	2
DCUs	Reset DET for I/P files	Output	0	0	1	1	1	1	1	5
	TOTAL # OF SENSORS:		15	16	4	4	4	4	4	51

Exhibit 3.2b: Future Installation I-15 RLCS Field Device and Sensors

3.1.2. External System Interfaces

All external systems shall retrieve RLCS status from a server outside the RLCS network. (outside a firewall). A single data file will include the following data elements:

3.1.2.1. Status (e.g.: open northbound, open southbound, closed)

3.1.2.2. Customers (e.g.: RLCS/FasTrak only, all traffic)

3.1.2.3. Access (e.g.: location 1 open, location 2 closed)

3.1.2.4. Signs (e.g.: Sign 1 “Express Lanes Open”, Sign2 “Express Lanes Closed”)

3.1.3. Communications interfaces

There are two external communications interfaces with the RLCS Application
:

3.1.3.1. The first is a connection to a Department of Transportation ISSC resource (possibly a WAN connection) via a firewall. All external systems will access RLCS data through this interface. This interface is a one-way output only interface.

3.1.3.2. The second consists of a secure remote dial-in interface through a firewall via a dial-up modem. This is a two-way interface that allows connection into the RLCS network via a remote computer equipped with the application software, and with a user logon authorized for remote access.

3.2. Functional requirements

This section describes the fundamental actions that must occur to accept inputs and produce outputs. It includes explanations of validity checks on inputs, [vendor must complete the validity check information] sequences of operations, and responses to abnormal situations.

See Appendix C for a collection of analysis diagrams that supplement this section.

3.2.1. Graphical User Interface (GUI)

The system shall have a Graphical User Interface (GUI) that allows the operator to view system status, issue commands to change device status, configure the system, export log data, and generate reports.

Input Entities (from list of entities and attributes in 3.4 Logical Database Requirements): All entities.

Output Entities: All entities.

3.2.1.1. The RLCS software shall have a logon screen for the GUI.

3.2.1.1.1. The logon screen shall request user name and corresponding password.

3.2.1.1.2. The logon screen shall activate command control for the user if the user requests it and has authorization.

3.2.1.1.3. Command control shall be from only specified workstations.

3.2.1.1.4. If command control is enabled by another user, and the logging in user is of higher security, the logging in user shall be requested to accept or deny command control.

3.2.1.1.5. If another user is logged in with command control and the new user takes command control, the other user is notified

3.2.1.2. Time Stamp, User, and Workstation ID Window

The GUI shall indicate the current date and time, user's name, and workstation location name. The GUI shall also show other users currently logged in the other units within the RLCS network.

3.2.1.3. Control/Monitor Command Entry Screen

3.2.1.3.1. The GUI shall provide an option that allows the system user to issue commands that monitor and control opening and closing events.

3.2.1.3.2. Based on the user's security level, the control option shall provide the user with the appropriate level of control.

3.2.1.3.3. The control option shall provide the user with the capability to set the operational status of failed devices.

3.2.1.3.4. The RLCS software shall display information about active overrides: Which are active, and which devices have no currently active 'rules protection' against erroneous opening/closing.

3.2.1.4. The GUI shall provide a display of the I-15 Reversible Lane Control System facility geographic area, including a layout of the mainline I-15, SR-163 freeway area in the same geographic area as the I-15 Reversible Lane. Screen information includes:

3.2.1.4.1. Facility status (e.g. 'Open' or 'Closed'.)

3.2.1.4.2. Current direction of traffic flow.

3.2.1.4.3. Customer eligibility (e.g. 'RLCS and FasTrak Only', 'All Traffic')

3.2.1.4.4. Current facility boundaries extending one mile in either direction.

3.2.1.4.5. Device sensor status using dynamic icons for all field device sensors and controllers.

3.2.1.4.6. For alarm status, the GUI shall also issue an audible alarm, and the icon shall be different from the okay status for that device. The visual alarm shall include a change of color for the affected device.

3.2.1.4.7. There shall be an option to turn off the audible alarm permanently or temporarily for a given period.

3.2.1.4.8. The alarm icon shall change to the normal status icon automatically when the alarm condition is removed. Alarm conditions shall be configurable on the screen.

3.2.1.4.9. When a device status has been overridden, on the screen it shall appear with different color from the normal and alarm status colors.

3.2.1.4.10. Status information shall continue to display when no user is logged on to the workstation and shall continually be updated every 2 seconds.

3.2.1.5. System Configuration Screen

3.2.1.5.1. The GUI shall provide an option for "Configuration" that is only accessible by the RLCS Software user with System Administrative privileges. It shall display and allow modification of all database tables with the exception of log tables.

When the system administrator modifies the database tables, the GUI shall analyze the data before storing in the database and notify the system administrator of any conflicting or redundant entries.

3.2.1.5.2. The configuration option shall allow a security level and password to be assigned to each defined staff member.

3.2.1.5.3. User security levels shall be assigned at the command level, device, mode, workstation, and system function.

3.2.1.5.4. The configuration option shall also allow user accounts l to be changed remotely in the field units.

3.2.1.5.5. When an operator is making changes on the system, the GUI configuration screen shall display to the user which device, controller, or workstation in the RLCS network will be affected by the changes. For example, when the user is making a changes in Pressure Calibration Parameters, it should be made clear which units will be affected.

3.2.1.5.7 The option to configure device rules shall require an additional login password for that option.

3.2.1.5.8 The GUI shall allow devices to be added and removed from the display without requiring programming effort.

3.2.1.5.9 The GUI shall allow the facility map to be modified without requiring programming effort.

3.2.1.6. Display/Export System Information Logs

The system shall display information logs and provide the capability to export the logs in common ASCII text for importing to commercial database, spreadsheet, or reporting programs. The following logs are required.

3.2.1.6.1. Device Command Log

3.2.1.6.2. System Operation Command Log

3.2.1.6.3. Problem Work Order Log

3.2.1.6.3.1. The Problem Work Order shall be a separate display that allows the user to enter information about a system problem.

3.2.1.6.3.2. The Problem Work Order data shall be editable and exportable to ASCII delimited files by the user.

3.2.1.6.4. Alarm Log (Critical and Warning Alarm)

3.2.1.6.5. Operator Daily Diary Log

3.2.1.6.5.1. The “Daily Diary” shall be a separate display that allows the user to enter free form text comments.

3.2.1.6.5.2. The user should not be able to update log entries other than for their own login, for the current day and current shift.

3.2.1.6.6. Maintenance Log

3.2.1.6.7. System Operation Schedule log

3.2.1.7. Single Device Status Screen

The GUI shall provide the ability to display the status of one device at the detail level, showing all sensor data for that device.

3.2.1.8. Device Category Status Screen

The GUI shall provide the ability to display the current status of a category of devices at the detail level, showing all sensor data for all devices of the same category. A category is all devices of the same category, such as gates, pop-ups, and CMS devices.

3.2.1.9. Report Screen

The user shall be able to retrieve historic reports from the COTS reporting system based on date range and report name.

3.2.1.9.1. Display/Modify parameters for the “Current Command Summary Report”

3.2.1.9.2. Display/Modify parameters for the “Event Log Report”

3.2.1.9.3. Display/Modify parameters for the “Current System Status Report”

3.2.1.9.4. Display/Modify parameters for the “Schedule Report”

3.2.1.9.5. Display/Modify parameters for the “Failure Summary Report”

3.2.1.9.6. Display/Modify parameters for the “Current Command Report”

3.2.1.9.7. Display/Modify parameters for the “Current User Report”

3.2.1.9.8. Display/Modify parameters for the “Safety Report”

3.2.1.9.9. Display/Modify parameters for the “Operations and Maintenance Report”

3.2.1.9.10. Display/Modify parameters for the “External Systems & Benefits Report“

3.2.1.9.11. Display/Modify parameters for the “System Status Report”

3.2.1.9.12. Display/Modify parameters for the “Inventory Report”

3.2.1.9.13. Display Report Results

3.2.1.9.14. Display/Modify Printer Setup

3.2.1.9.15. Display/Modify Report Schedule

3.2.1.9.16. Print/Save Report Results

3.2.1.10. Emergency Notification Information Screen
The system shall display the appropriate emergency contact information in the event of an alarm condition.

3.2.1.11. Command Confirmation/Abort/Override Screen
The GUI shall display a separate window requesting confirmation of the command upon receiving a command either from the user at the keyboard, or from a scheduled sequence of commands.

3.2.1.12. Alarm Acknowledgment/Silencing Screen
The GUI shall allow the operator to acknowledge an alarm and have the option to silence the audible portion of the alarm for a configurable number of seconds or permanently for that device only.

3.2.1.13. The GUI shall include diagnostic screen providing the user with the capability to diagnose failed devices at the sensor level.

3.2.1.14. Change System Mode
the GUI shall provide a screen for authorized users to change system mode.

3.2.1.15. Help Screen
The GUI shall provide a screen for describing system features, functions, database tables, and fields.

3.2.2. Process Monitoring and Control

The RLCS software will monitor the status of all field devices and will process requests for changing field device status.

Input Entities (from list of entities and attributes in 3.4 Logical Database Requirements): Alarm Type, Command Level, Device, Device Alarm Criteria, Device Command, Device Rules, Device Status, Diagnostic Command, Location, System Control Parameters, System Mode, System Operation Status, System Operational Command

Output Entities: Alarm Type, Command Level, Device, Device Command, Device Command Log, Diagnostic Command, Location, Operator Daily Diary Log, System Operation Command Log, System Operation Command Log, System Operation Status, System Operational Command

3.2.2.1 The RLCS shall monitor all field device sensors, and shall process operator requests for changing field device status.

3.2.2.2 Any operator or system command, which changes the state of field control devices, must be checked for integrity at multiple levels in the RLCS.

3.2.2.3 The RLCS software shall monitor, display, and update the database with the status of all system field elements. Any change in device state shall be reported on the screen not later than 2 seconds from the time it occurs. In addition to monitoring field devices the system shall also monitor field controllers and connected on the RLCS network for control system integrity. The system shall report any users logged in RLCS network computers any time and all commands issued in the field units.

3.2.2.4 During 'degraded' mode, the system shall monitor device sensors at the frequency rate stored in the database to take effect only during 'degraded' mode. In general, the system shall monitor the status of all field devices at the frequency specified in the System Control Parameters for that mode.

3.2.2.4.1 The system shall control all system field elements to device sensor level for those device sensors that may be controlled. For example, the temperature sensor at the controller cabinet is not a controllable sensor, whereas the 'gate arm control lines' sensor may be controlled.

3.2.2.4.2 Each device control command shall check the current status of all closure devices in the system and shall abort if any closure control device status is unknown.

3.2.2.4.3 Each command (at the device sensor command, device command(macro), or system operational command (super macro) level) shall only be executed when a valid or good status exists for all device sensors. An authorized user shall be able to log in and issue device status requests and control commands from specified computers in the network. (This is determined

based on the user's access level and authorized workstations.)

3.2.2.4.4 The current status for all devices shall be maintained at each controller unit.

3.2.2.4.5 Alarms
Check Device Status for Alarm Condition
Each status received from device sensors shall be checked against alarm conditions for that device sensor and the status will be updated to indicate an alarm.

3.2.2.4.6 Critical alarms shall be generated when one or more of these conditions are met.

1) A closure device changes from a known state to unknown state (status lost)
2) A closure device changes from legal state to illegal state. E.g. pop-ups in the down position when they are supposed to be up.
3) The control system Integrity verification indicates a verification failure.
4) When a user logs in any of the field units.
5) When a command to override a device has been issued anywhere in the system.
6) When there is a communication failure within the RLCS network
7) When a computer in the RLCS network goes down
8) Power failure at any controller or workstation
9) When a cabinet ID is changed.
10) When the DCUs are in manual mode.
11) Watch Dog timer failure

3.2.2.4.7 Warning alarms shall be generated when one or more of these conditions are met.

1) security sensor activation at either the FCU or DCU.
2) When Air pressure, Temperature in cabinets, and Voltages are outside the limits of established thresholds as stored in the database.

3.2.2.4.8 If a critical alarm occurs during opening or closing operation, the system shall present the operator with possible actions that can be taken in order to complete the operation. If overriding a device status is needed in order to proceed, the system shall determine if the operator has high enough security and provide advise on how to proceed.

3.2.2.4.9 Process GUI Commands

3.2.2.4.9.1 In order for a command to be processed from any workstation or controller, the MCU field device shall be in the "Auto" mode.

3.2.2.4.9.2 The system operator shall be able to override any device and continue with a system operational command sequence. To 'override' a device means to set the status to a normal value even if the device is not functioning in order to continue with a sequence. Field staff would manually operate any device that is not responding to a controller

command prior to the operator 'overriding' the device status.

3.2.2.4.9.3 The process of overriding a device status shall not affect the status of any other device.

3.2.2.4.9.4 Business Rules / Interlocks / Safety Screening
Each control command that is processed must be validated against the secured safety rules (stored in non-volatile memory) for the command. For example, if the operator issues a command to open the south gate while the north gate is open, the RLCS software will determine that opening the south gate cannot occur when the north gate is open, and will give an indication that the operation cannot be completed. The validation will occur at each control unit in the system that receives the command.

3.2.2.4.9.5 Commands are only forwarded from superior units to inferior ones. This prevents a lower level unit from changing the state of a device which is controlled by either a higher level unit, or by a peer unit. The TSU is superior to the FCUs which are superior to the DCUs.

3.2.2.5 Track and log all Failed Requests for Device Status and Control

3.2.2.5.1 If a status from any device is not received upon request, the system shall automatically request the status again.

3.2.2.5.2 Failure to receive a valid status after a configurable number of retries shall be considered a device failure.

3.2.2.6 Identify units and Initialize all Devices

3.2.2.6.1 When each workstation and control unit (workstation or intelligent controller at the FCU or DCU) comes online, the system shall identify it and all its associated device sensors.

3.2.2.6.2 The RLCS software shall initialize each control unit and device sensor as it is identified.

3.2.2.6.2.1 RLCS Software Startup PROCESS: The RLCS software in the field shall first identify the its unit when it starts, by reading the cabinet id. The RLCS software will then proceed to make sure that all the cards required in that unit are present and working properly. The RLCS software will do a control system integrity check (see requirement 3.0.9) and initialize all the specified tables. If everything is OK the start up process shall not exceed 30 seconds. The RLCS software shall then monitor all the devices and send the current status to the FCU or TSU every 2 seconds (or at the rate specified in the System Control Parameters for the current mode).

3.2.2.7 The RLCS software shall be designed to allow for future changes to the roadway without requiring programming effort. Updating non-volatile memory-based tables shall be sufficient to accommodate future changes to the roadway. Some examples of future changes to the facility include, change in the number of closure devices. change in the number of entrances to lanes, change in the number of changeable message signs, Different closure devices, and different operational procedures.

3.2.2.8 Collect Log Data

The system shall generate log files as follows for reports:

3.2.2.8.1 Device Command Log: Contains device commands issued with time stamp, operator ID, unit where the command was issued at and shall include failed or aborted commands. Device command log shall not be editable by users.

3.2.2.8.1.1 System Operation Command Log: Contains system operational commands issued with time stamp, operator ID, unit where the command was issued at and shall include failed or aborted commands. System Operation command shall not be editable by users

3.2.2.8.1.2 The Problem Work Order Log will be generated automatically with failure information at the time of failure. Some input fields in this log will allow the operator to input status and emergency notification information.

3.2.2.8.1.3 Alarm Log will contain information about warning and critical alarm events.

3.2.2.8.1.4 The Daily Diary Log will be generated automatically when a user with Operator authority logs on to the system. Some input fields in this log will allow the operator to input free form text information.

3.2.2.8.1.5 Special Event Log: This log will contain information about scheduled special events.

3.2.2.8.1.6 System Operation Schedule Log: This log contains information about scheduled operations.

3.2.2.7.1

3.2.3 Sequencing

Input Entities (from list of entities and attributes in 3.4 Logical Database Requirements): Alarm Type, Command Level, Device, Device Alarm Criteria, Device Command, Device Command Macro, Device Command Steps, Device Rules, Location, System Control Parameters, System Mode, System

Operation Command Schedule, System Operation Status, System Operational Command Steps, System Operational Command.

Output Entities: Device Command Macro, System Operational Command

3.2.3.1 The RLCS shall execute stored operational control command sequences based on the current system mode of operation and the schedule for each sequence. The operational control command sequences to be stored and executed with the initial configuration of the system are listed in Appendix F

3.2.3.2 The RLCS shall present scheduled command operations to the operator at the GUI for confirmation prior to executing the command.

3.2.3.3 At any point in an opening or closing sequence, the sequence shall be halted if:

3.2.3.3.1 A device fails to report completion of the current sequence step within the response time window allotted for the step, or

3.2.3.3.2 The status of a closure device, which was previously opened at the current entrance, changes to ‘unknown’ or ‘closed’, without an operator-initiated command.

3.2.3.3.3 The status of a closure device, which was previously closed at the current entrance, changes to ‘unknown’ or ‘open’, without an operator-initiated command.

3.2.3.4 At any point in an opening sequence, the sequence shall be halted if the status of a closure device for the opposite direction of travel changes to ‘unknown’ or ‘open’.

3.2.3.5 To resume an opening or closing sequence after a halt has occurred, the operator shall be able to issue a command to resume if the offending device status can be corrected within a configurable time period as defined in the database and in non-volatile memory.

3.2.4 Data Processing and Security

The RLCS shall store, process, and retrieve all data necessary to operate the application software as well as generate current and historical reports of system operations, and export system status data to an external server data store. The RLCS shall also store, process, and retrieve all data necessary to secure the system from unauthorized use. A commercial off-the-shelf database management system shall be used for this function.

The RLCS database stores information needed to operate the RLCS as well as historical transaction data to generate reports of system operations.

Input Entities (from list of entities and attributes in 3.4 Logical Database Requirements): All entities

Output Entities: All entities

3.2.4.1 The RLCS application software shall update and read database tables to support system operations.

3.2.4.2 The RLCS application software shall Update and read password and device rule data in encrypted format.

3.2.4.3 Update and read Security information
The Personnel Security Level entity stores information about the five attributes used to restrict access to the RLCS: Command Level, Device, Mode, Workstation, and System Functions.

3.2.4.4 Command levels are of three types: 'Status Only', 'Control', and 'Override'. Users with 'Status Only' command level security may not issue any control commands at any level (device, macro, or super macro). 'Control' allows a user to issue control commands, and is a higher level of security. 'Override' allows a user to temporarily change the status of a device in the database for a configurable period of time in order to allow a command sequence to continue.

Commands shall be classified in these categories

(1) Device control commands. These are single commands that change the state of a device. Example: Raise gate at location 1

(2) Device Macro Commands. This is a group of two or more sequentially executed commands that change the states of two or more closure devices. Example Close CMS 1 through 4.

(3) Super Macro Commands. This is a group of two or more sequentially executed macros that change the states of an Entrance. Example Close South end Location 2.

(4) Override Commands. These are commands that force the status of a device to a temporary known state for the purpose of completing an operation which otherwise

would not be completed if the device remained in an unknown state. This type of command changes the database value for the device only and does not send a device command to the field device.

(5) Device Status Commands. These are commands that request the status of a device. Example Get status of DCU1, or get the status of CMS12.

(6) Diagnostic Commands. These are commands that run diagnostic on devices or controllers. Example: Run diagnostics on the communication card in DCU1.

3.2.4.5 The system shall will employ a one-way hash function as an aid to maintaining the integrity of the data and software in the field. The hash value returned by the function shall will be at least 128 bits in length. The MD5 algorithm is acceptable for this purpose.

3.2.4.5.1 At each time, one or more of the above item types, listed under 'Control Unit Non-Volatile Memory', is created or modified, a UTC date/time stamp shall will be updated. The update of the time stamp shall will be the last step in the process which builds the time stamped code/data section.

3.2.4.5.2 The system shall will also, for each control unit in the system, produce a table of the returned 'one-way hash function' (Message Digest) values, of each of the 'Control Unit Non-Volatile Memory' items. The returned 'Message Digest' values shall will be stored as hexadecimal characters. The appropriate 'Message Digest' table shall will be maintained in non-volatile memory in each system control unit.

3.2.4.5.3 The system will provide for periodic verification that current, recomputed 'Message Digest' values, for each unit in the system, correspond with 'record' values computed by the development processMD5 algorithm. The periodic evaluation shall will occur at least once a day. The 'Message Digest' value verification results shall will be recorded in the system log. A verification failure shall will cause an alarm condition for the affected control unit. If the failure occurs in checking the non-volatile memory items, the system shall will prevent the affected unit from being used in control sequences.

3.2.4.5.4 The system shall will provide for 'Message Digest' verification requests for a given unit by operator command.

3.2.4.5.5 For system login purposes, the hash function shall will also be used to encrypt user passwords. [Harrison to ask Don Day why these are requirements.]

3.2.4.5.6 To change device command rules on the production system, the System Administrator must upload a new database version after testing the rule changes in the Simulator environment.

3.2.5 Reporting

The system will use data exported from the RLCS database to create and format a variety of reports. A commercial off-the-shelf reporting tool shall be used for this function.

Input Entities: All RLCS log data and any other entities exported to the COTS reporting tool.

Output Entities: None to RLCS database, only output reporting parameters to COTS reporting package data store, and report output to display, print, or file storage.

3.2.5.1 Format Report for GUI Display

3.2.5.2 Format Report for Print/Export Output

The following reports are representative of the reports to be produced by the system. Other reports could be produced from the data stored in the database.

3.2.5.3 Create “Current Command Summary Report” from System Command (Super Macro), Device Command (Macro), Device Sensor Command, Device Sensor Rules, Device Rules, System Operation Schedule, and System Operational Command Sequence Schedule entities.

3.2.5.4 Create “Event Log Report” from “Device Sensor Command Log”, “Device Command Log”, and “System Operation Command Log” entities.

3.2.5.5 Create “Current System Status Report” from System Operation Status Log entity for the current time.

3.2.5.6 Create “Schedule Report” from the “System Operational Schedule” entity.

3.2.5.7 Create “Failure Summary Report” from “Device Sensor Command Log”, “Device Command Log”, and “System Operation Command Log” entities, for status value indicating a “failure”.

3.2.5.7.1 The system shall generate problem reports based on alarms and system status reports

3.2.5.8 Create “Current User Report” from “Personnel Status” entity.

3.2.5.9 Create “Safety Report” from “Device Sensor Rules” and “Device Rules” entities.

3.2.5.10 Create “Operations and Maintenance Report” from “Device” entity using ”Last Maintenance Date” attribute.

3.2.5.11 Create “System Status Report” from the ‘System Operation Status Log’ entity for a specified time period.

3.2.5.12 Create “Inventory Report” from “Device”, “Device Status”, “Device Category”, and “Location” entities.

3.3 Performance

3.3.1 External Interfaces

Priority: Must have

3.3.1.1 The external server data store containing RLCS status for use by external systems shall be updated once per minute.

3.3.1.2 The field device status information logging to the database shall be 2 seconds, but can be configurable within the database to more than 2 seconds by the user.

3.3.1.3 The field device status information display update frequency shall be 2 seconds, but can be configurable within the database to more than 2 seconds by the user.

3.3.1.4 The RLCS shall receive device status information from devices sensors within 2 seconds of the status information being issued by the device sensor.

3.3.1.5 Field devices shall receive respond to commands from the RLCS within 12 seconds of the command confirmation being issued by the operator using a keyboard (or other input device).

3.3.2 User Interface (GUI)

Priority: Must have

3.3.2.1 The RLCS shall support multiple users logged on, up to the limit of the number of users defined in the database.

3.3.2.2 Not including device and network response times, requests from the GUI for status updates shall not exceed 2 seconds to update the GUI display.

Not including device and network response time, requests from the GUI for device status changes (control commands) shall not exceed 2 seconds.

3.3.2.3 The facility map on the screen shall refresh every 2 seconds but can be configurable within the database to more than 2 seconds by the user.

3.3.2.4 The RLCS notification to the operator workstation of any critical alarms shall occur within 2 seconds of alarm detection, and shall occur whether or not an operator is logged on to the system.

3.3.3 Process Monitoring and Control

Priority: Must have

3.3.3.1 The field units (controllers) shall continually monitor device status, controller status and the control system integrity and send the status to the central

computer in the TMC every 2 seconds or less.

3.3.3.2 The RLCS shall detect alarm conditions within 2 seconds of occurrence.

3.3.4 Sequencing

Priority: Must have

3.3.4.1 At a minimum of every 60 seconds, the system shall check the current date and time against a list of scheduled events for the current mode to determine if any event should be executed.

3.3.4.2 The RLCS shall support at a minimum the 4 daily 'normal' mode open and close scheduled operations plus at least the same number of 'emergency' and 'maintenance' mode scheduled events.

3.3.5 Data Processing and Security

Priority: Must have

The database retrieval and update response time shall not impact any other performance requirements such as the GUI response time or monitoring and control responses. In other words, the database performance is a component of the total response time for any other performance requirement. If the GUI is required to reflect change in status within 2 seconds, then the database update time must be less than 2 seconds.

3.3.6 Reporting

Priority: Must have

3.3.6.1 The operator shall be able to store and retrieve previously created report results from the RLCS for a minimum period of 60 days, but configurable for up to one year.

3.3.6.2 The raw data used to create reports shall be kept in the RLCS for a minimum period of 13 months prior to backing up to tapes or other secondary storage media.

3.3.6.3 Report processing shall not impact any other performance requirements such as the GUI response time or monitoring and control responses

3.3.6.4 Report response time shall be determined by the database resources allocated to the reporting function. Depending on user needs for fast report response times (such as for ad hoc reporting), database extracts may be created for reporting purposes only.

3.3.7 Communications

Priority: Must have

3.3.7.1 RLCS system components will communicate via the private communications networks established by Department of Transportation District 11 prior to the development of the RLCS. Any operator or system command, which changes the state of field control devices, must be checked for integrity at multiple levels in

the system. Valid checksum algorithms must be employed to check the integrity of messages between units.

3.3.7.2 The RLCS must support the following data transfer performance goals:

The number of kbits transmitted for a single polling event of all device sensors is estimated to be:

# of sensors x bytes/status command x 8bits/byte x 1k/1000=
205 x 200 x 8 x 1/1000= 328 kbits

The transmission rate required to transfer this data in 2 seconds is: 328 kbits/2 sec. = 164 kbits/s
At a 30 second polling interval, the transmission rate drops to 10.9 kbits/s.

# of Sensors*	Bytes per status command	Polling Interval	Transmission Rate (kbits/second)
205	200	2	164
205	200	30	10.9

*The # of sensors is the total # of sensors in **Exhibit 3.2a** and **Exhibit 3.2b** combined.

Polling all system devices constitutes the majority (over 99.99%) of transactions on the network. The opening and closing sequences that occur four times daily, add only a small fraction to the total system load.

At 164 kbits/s, in a 24-hour period, 14,169,600k bits will travel over the network:

(164 kbits/sec) x (60 sec/min) x (60 min/hr) x (24 hrs/day) = 14,169,600k bits/day

The following chart shows the number of kbits added by the daily opening and closing operations, which represent only 0.009% of the daily system load: (1,312 / 14,169,600 = 0.00009)

# of Sensors	Bytes per control command	# of control commands per day	Total k bits for control commands
<205	200	4	(200*205*4*8)/1000 = < 1,312 k bits

3.4 Logical Database Requirements

The RLCS database stores information needed to operate the RLCS as well as historical transaction data to generate reports of system operations.

The entities in the table below fulfill the functional requirements of the RLCS, but the list does not include any data that might be included with a vendor's pre-packaged COTS system or custom-designed solution. Additional data entities required for design or included with a COTS system are not disallowed by this specification.

#	Entity Name	Minimum Attributes
1	Agency	Agency ID, Agency Name, Contact, Address, Phone
2	Alarm Type	Alarm Type ID, Description (critical, warning)
3	Command Level	Command Level ID, Name (examples: status, control, override), type(status/control)
4	Customer Type	Customer Type ID, Name (examples: general public, FasTrak , HOV)
5	Device	Device ID, Name, Device Status ID, graphic image for display, location ID, direction, Device Category ID, Last Maintenance Date
6	Device Alarm Criteria	Device Alarm Criteria ID, Device ID, Alarm low range, Alarm high range, Alarm Description, Device Status ID
7	Device Category	Device Category ID, Name, Description of category
8	Device Command	Device Command ID, Device ID, Command String, Timeout, Command Level
9	Device Command Macro	Device Command Macro ID, Device ID, Command Name, Command String, Timeout, Command Level
10	Device Command Log	Device Command Log ID, Device Command ID, Date, Time, Device Status ID, Operator ID
11	Device Command Steps	Device Command Steps ID, Device Command ID, Step #, Device Command
12	Device Rules	Device Rules ID, Mode, Device X desired status, Device Y prohibited status
13	Device Status	Device Status ID, Name, Description of status (e.g. ok, alarm)
14	Diagnostic Command	Diagnostic Command ID, Name, Diagnostic Program Path and Name, Command Level
15	Emergency Notification Profile	Emergency Notification Profile ID, Schedule Shift, Alarm Type ID, Personnel ID, Pager #, Telephone #
16	Location	Location ID, Highway #, Segment, Direction, Lane #, geo code, Name
17	Operator Daily Diary Log	Operator Daily Diary Log ID, Personnel ID, Date, Notes
18	Personnel	Personnel ID, Name, Initials for login, password, password date
19	Personnel Classification	Personnel Classification ID, Name, Description of classification
20	Personnel Security Level	Personnel Security Level ID, Mode, Functions, Command Level, Devices, Workstation
21	Personnel Security Level Device	Personnel Security Level ID, Device ID
22	Personnel Status	Personnel Status ID, Name, Description of status (active & logged on, active & logged off, inactive)
23	Personnel System Functions	Personnel ID, Function ID
24	Personnel System Modes	Personnel ID, System Mode ID
25	Personnel Workstations	Personnel ID, Workstation ID
26	Problem Work Order	Problem Work Order ID, Date, Time, Operator, Problem Work Order Status ID, Description
27	Problem Work Order Personnel	Problem Work Order ID, Personnel ID
28	Problem Work Order Status	Problem Work Order Status ID, Name, Description of status
29	Problem Work Order Type	Problem Work Order Type ID, Name, Description of type
30	Report Parameters	Report Parameters ID, Report name, Report number, Report begin date, Report end date
31	Sign Message	Sign Message ID, Name (e.g. "Express Lanes Open", "Express Lanes Closed")
32	System Control Parameters	System Control Parameters ID, System Mode ID, Login retry count, Polling rate, Override timeout, Max users, Display colors, Software version, Database version, Username length, Password length
33	System Functions	System Functions ID, Function Name
34	System Mode	System Mode ID, Name, (Normal, Degraded, Emergency, Maintenance, and others as defined)
35	System Operation Command Log	System Operation Command Log ID, Date, Time, System Operational Command ID, System Operation Status ID, Operator ID
36	System Operation Command Schedule	System Operation Schedule ID, Mode, Start day/time, End day/time, Frequency, System Operational Command ID or Device Command Macro ID, or Device Command ID. This entity can reflect items scheduled in advance that repeat at a set period, and can reflect items entered into the system for immediate execution.
37	System Operation Status	System Operation Status ID, Name (Open North, Open South, Closed), Customer Type ID
38	System Operational Command Steps	System Operational Command Steps ID, System Operational Command ID, Step #, Device Command
39	System Operational Command	System Operational Command ID, Name, Description, Timeout, Command Level

#	Entity Name	Minimum Attributes
	(super macro)	
40	Workstations	Workstation ID, Name, Location, Make, Model

Exhibit 3.3: I-15 RLCS Entities and Attributes

See the Entity Relationship Diagram and Relationship Descriptions in Appendix C for more details.

3.5 Design Constraints

3.5.1 Commercial Off-the-Shelf Software

3.5.1.1 The data processing and security, and reporting functions of the RLCS application software shall be implemented with commercial off-the-shelf software.

3.5.1.2 The data processing, security, and reporting functions as well as the server and client operating systems would preferably use the following:

- Oracle 8*i* for the database server and clients
- HP UX or Solaris server operating system (latest version)
- Windows NT or Linux for the client operating system (latest version)
- OS/9 or other real time operating system for the controller operating system
- Crystal Reports, Brio or comparable for reporting package
- CCC/Harvest or comparable for change and configuration management.

3.5.2 Security

The RLCS shall incorporate a database to store, process, and retrieve all data necessary to secure the system from unauthorized use. The processing code at the FCU and DCU controllers shall be resident in non-volatile memory .

3.5.2.1 The RLCS shall incorporate a database to store, process, and retrieve all data necessary to secure the system from unauthorized use.

3.5.2.2 The application software processing code and application software data such as login information at the FCU and DCU controllers shall be resident in non-volatile memory.

3.5.2.3 The MD5 algorithm shall be used to secure application data and software in the controllers and the application server.

3.6 RLCS Application Software Attributes

3.6.1 Reliability

3.6.1.1 The RLCS must demonstrate the ability to function continuously without needing to be reset or rebooted due to an RLCS error for at least 30 consecutive days.

3.6.1.2 Valid checksum algorithms must be employed to check the integrity of messages between units.

3.6.1.3 The RLCS must be built with redundant capabilities to ensure uninterrupted operation. The RLCS will function in a degraded mode in the following manner:

3.6.1.3.1 If the TMC workstations or network server fails, resulting in loss of field status at the TMC, alternate control shall be at FCU South or FCU North. The operator shall be able to dial in from a back up computer to either FCU North or FCU south and open and close the reversible lanes.

3.6.1.3.2 If FCU North or South fails: (FCU Controller failures or FCU-TSU communications failure) Loss of changeable messages signs and DCUs associated with the failed FCU. Alternate control at the non-failed FCU (North or South).

3.6.1.3.3 If FCUs North and South both fail: (FCU Controller failures or FCUs-TSU and FCU-FCU communications failure) Loss of changeable message signs 1-12 and DCUs 1-5. Alternate control units: Direct control at DCUs 1-5, and CMS 1-12 control from CMS cabinets. The operator shall be able to connect a lap top computer at the DCUs and operate the devices or perform manual operation from the MCU. The operator shall also be able to connect a lap top on the CMS cabinet and control the signs or perform manual operation of the signs from the cabinet.

3.6.1.3.4 If any DCU 1-5 fails: Field devices related to the failed DCU. Alternate control unit: MCU and manual control at the field devices.

3.6.1.3.5 If any MCU fails: Loss of field devices. Alternate control unit: Manual control at the field devices related to the failed MCU. The devices can be manually controlled/operated from their cabinets (e.g.: Gates)

3.6.1.4 The current configuration information for each processing unit in the field shall be duplicated in a database at the TMC level.

3.6.2 Availability

Priority: Must have

The RLCS must be available 24/7, 365 days per year. The normal operating mode is Monday through Friday, between 5:00am and 8:00pm, but the system must be functional in order to stay in its closed state after hours. If there is a failure, recovery time must be no greater than 10 minutes, and total yearly uptime must be at least 99.99% (.01% downtime, or approximately 50 minutes per year).

3.6.3 Maintainability

Priority: Must have

3.6.3.1 The RLCS shall support remote system administration and maintenance of the system.

3.6.3.2 The RLCS shall utilize an open architecture that is modular and scaleable. The system will be scaled up to a maximum of two additional DCU controllers, each with the number of devices currently at DCU Location 1, plus four additional CMS, and

twenty additional contact closures)

3.6.3.3 Wherever possible open systems standards for hardware, software, software development tools, and communications shall be used.

.

Appendixes A - Traceability Matrices

The original System Requirements Document – Version C produced by TransCore in December 1998, was the basis for this Software Requirements Specification. The two tables referenced in this appendix show the migration of requirements from the original document to this document. If a requirement was not used because it was no longer valid, it is labeled 'OUT'. Some of the requirements in this Software Requirements Specification are new (not specified by the TransCore document), and therefore are not referenced in the matrix.

Additionally, some system requirements are not software requirements, and will be referenced in the Request for Proposals and System Architectural Design documents, but not in this Software Requirements Specification.

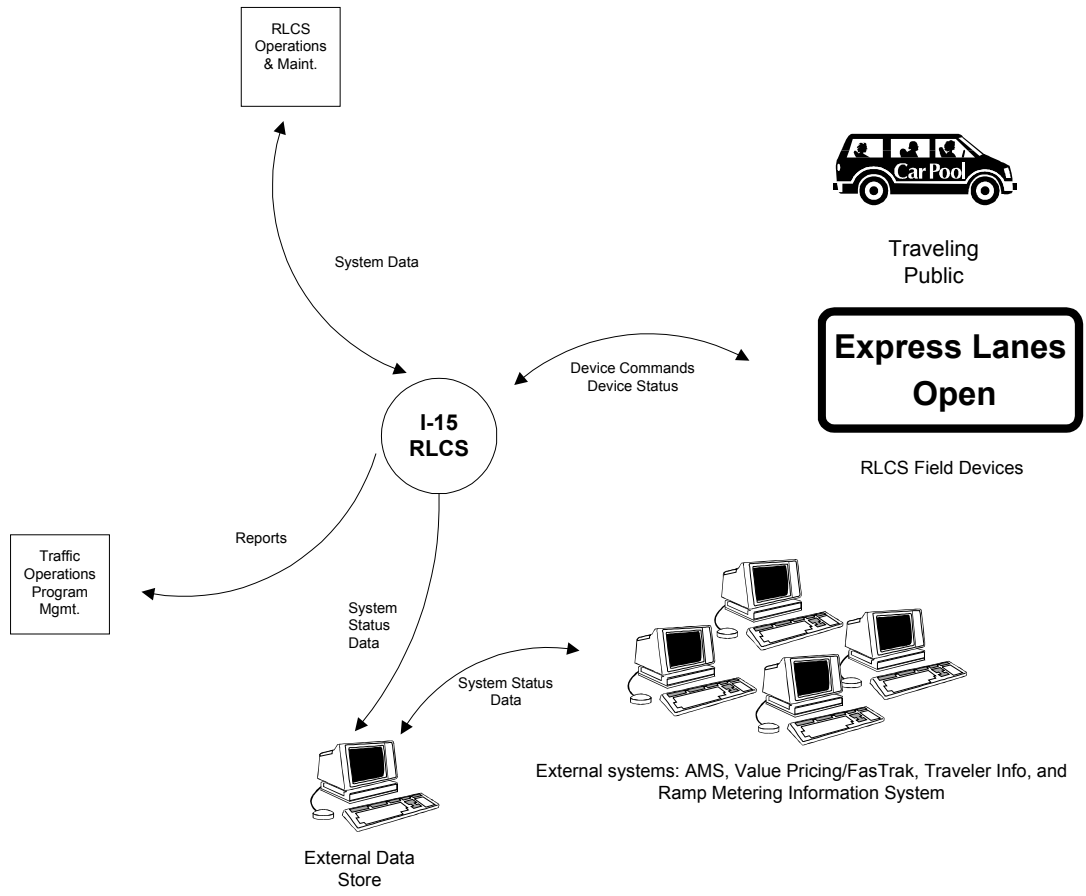
See SRSMatrixFromTransCore2.doc for the matrix in order by TransCore-produced system requirements.

See SRSMatrixFromVIP2.doc for the matrix in order by the VIP-produced software requirements.

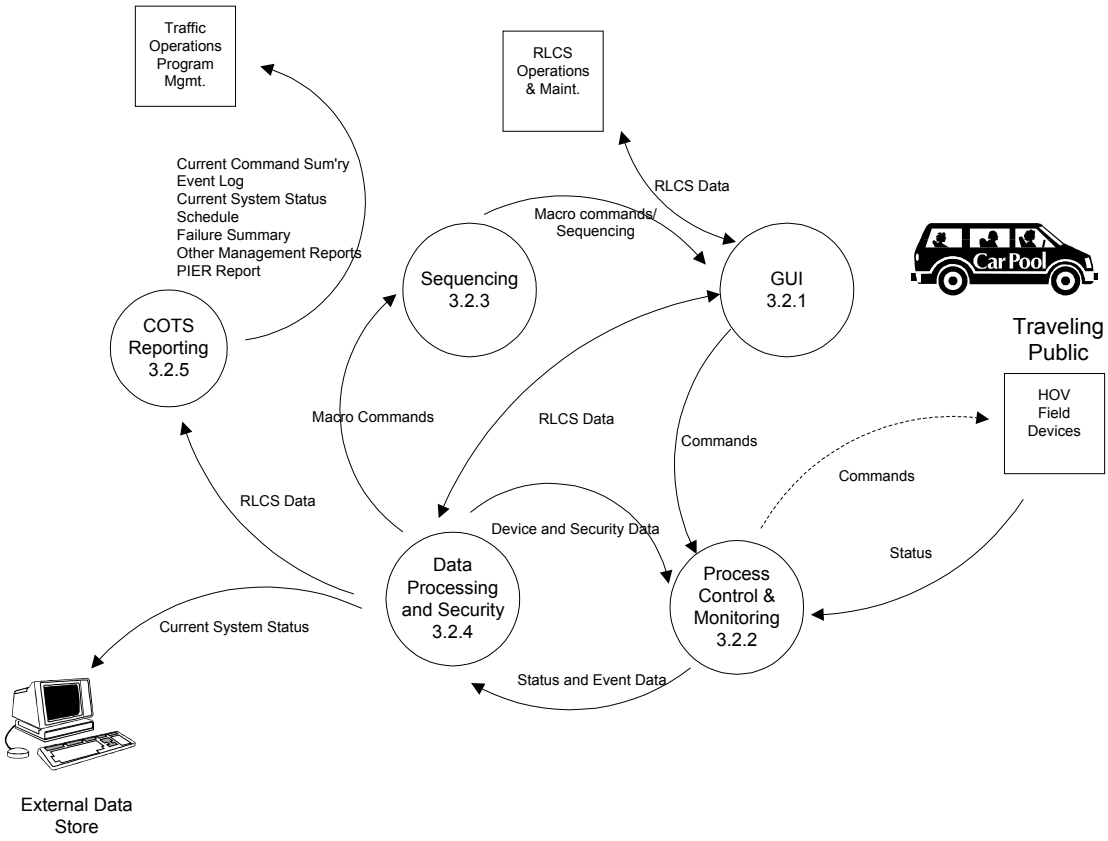
Appendix B – Terminology

Term	Definition
DCU	Device Control Unit
Device Override	The capability of the system to allow an operator with the proper security to continue an operating sequence through to the end even though any intermediate step resulted in a device control failure, by allowing the operator to input a device status thereby overriding the status coming from the field.
Facility	The I-15 reversible lane physical roadway, field devices, and electronic components and software used to monitor and control the field devices.
FCU	Field Control Unit
Field Devices	Gates, pop-ups, CMS, lights, loop detectors, power, pressure transducers, and any other controlled device.
MCU	Manual Control Unit
Operational Override	The capability of the system to allow an operator with proper security to issue device commands outside of a predetermined operational event, on demand.
PIER	Post Implementation Evaluation Review
RLCS	The I-15 Reversible Lane Control System. The electronic components and software used to monitor and control the field devices within the I-15 Reversible Lane Facility. Can refer to the existing or proposed RLCS.
TEES	Transportation Electrical Equipment Specification
TMC	Traffic Management Center
TSU	Traffic Systems Unit

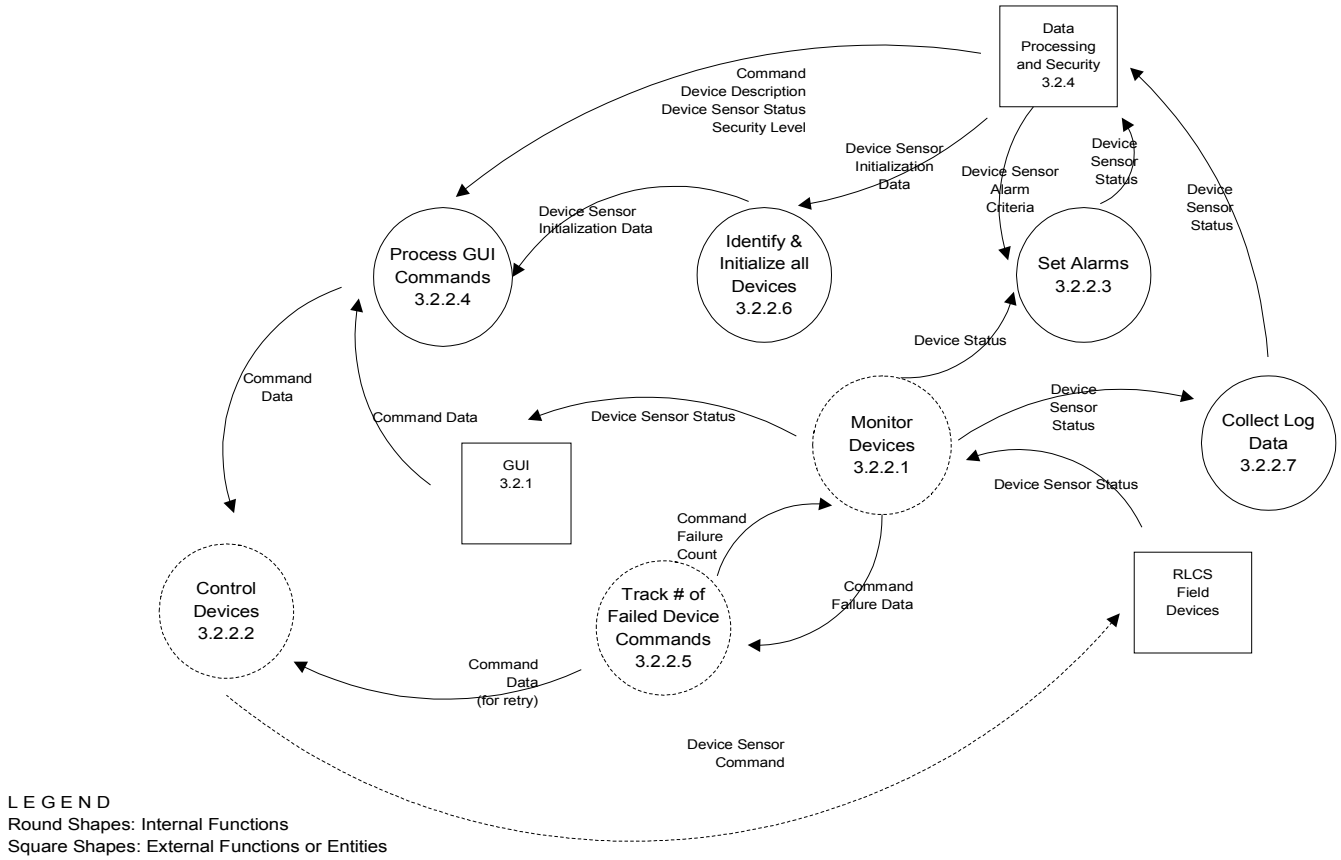
Appendix C – Data Flow Diagrams, and Data Model



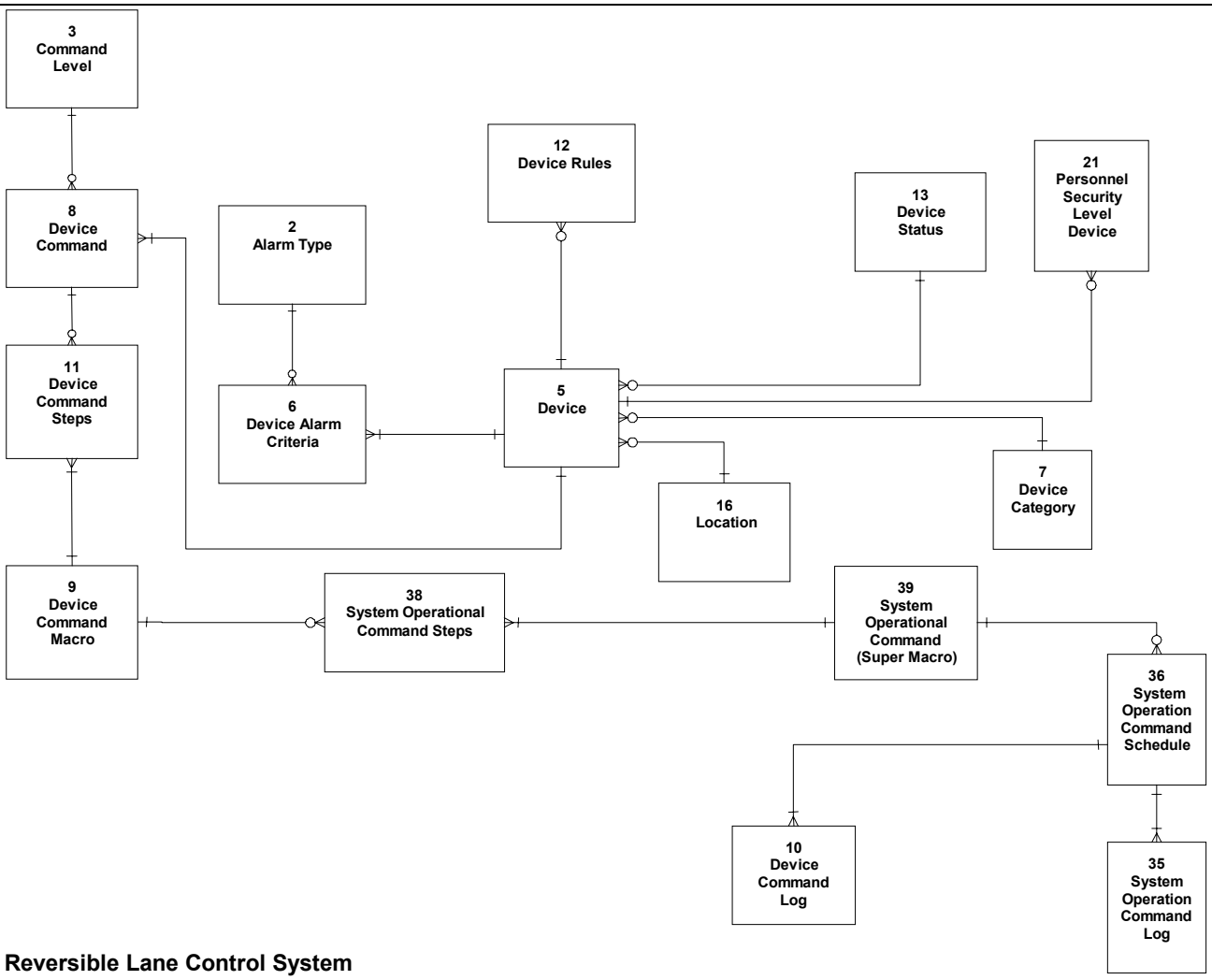
I-15 Reversible Lane Control System
Level 0 - Context Diagram



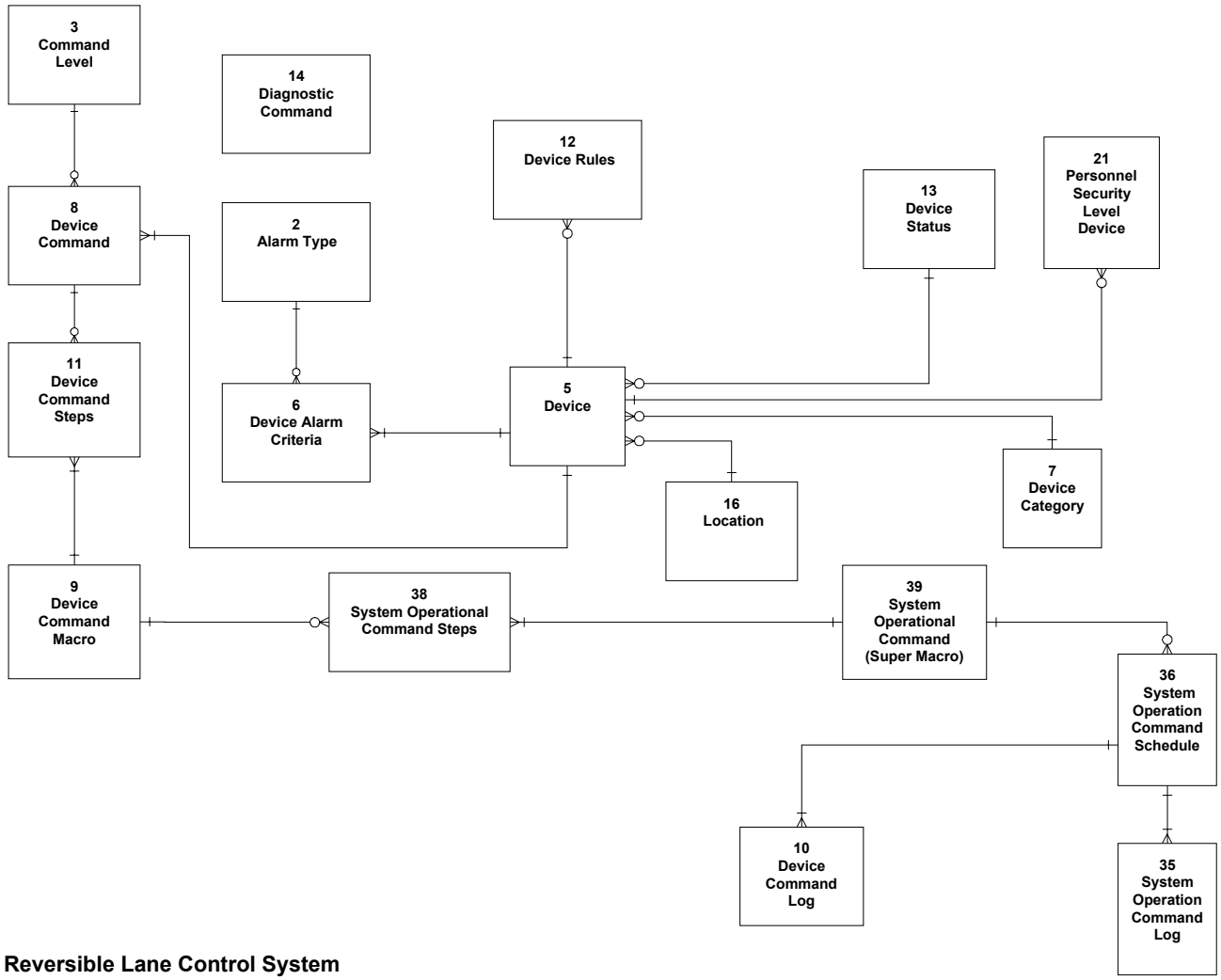
I-15 Reversible Lane Control System
Level 1 - Data Flow



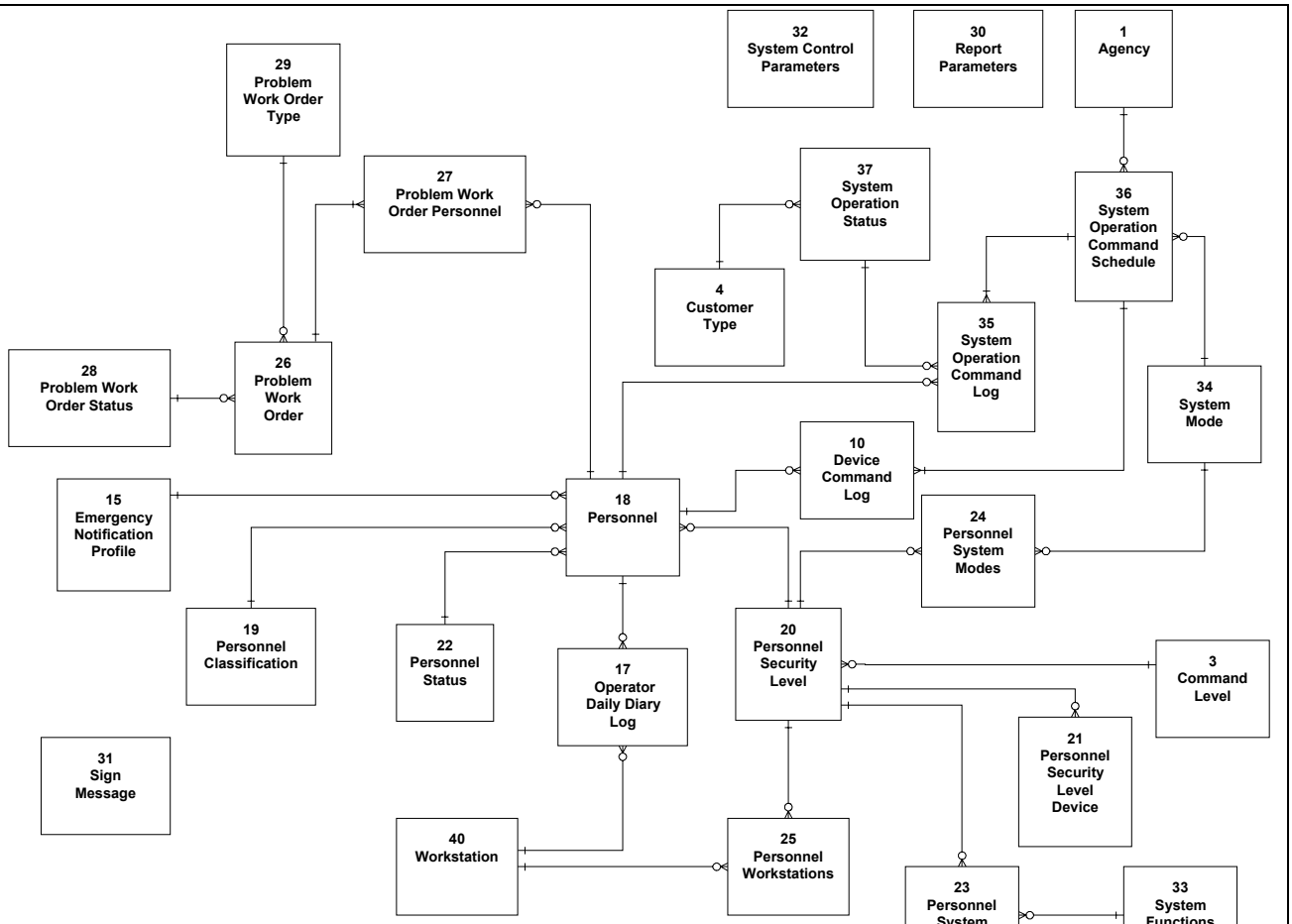
I-15 Reversible Lane Control System: Process Monitoring and Control 3.2.2
Level 2 - Data Flow



I-15 Reversible Lane Control System
Entity Relationship Diagram - Device and Command Related Entities



I-15 Reversible Lane Control System
Entity Relationship Diagram - Device and Command Related Entities



I-15 Reversible Lane Control System
Entity Relationship Diagram - Personnel, Work Order, and Scheduling Related Entities

#	Entity Name	Relationships
1	Agency	• Each Agency may be referenced in one or more System Operation Schedules
2	Alarm Type	• Each Alarm Type may be referenced in one or more Device Alarm Criteria
3	Command Level	• Each Command Level may be referenced in one or more Device Commands
4	Customer Type	• Each Customer Type may be referenced in one or more System Operation Statuses
5	Device	• Each Device has one Device Type • Each Device has one Device Status • Each Device has one Location • • Each Device may have one or more Device Rules • Each Device has one or more Alarm Criteria • Each Device has one or more Device Commands • Each Device may be referenced in one or more Personnel Security Level Device
6	Device Alarm Criteria	• Each Device Alarm Criteria is for one Device • Each Device Alarm Criteria references one Alarm Type
7	Device Category	• Each Device Category describes one or more Devices
8	Device Command	• Each Device Command refers to one Device • Each Device Command may be referenced in one or more Device Command Steps • • Each Device Command is described by one Command Level
9	Device Command Macro	• Each Device Command Macro has one or more Device Command Steps. • Each Device Command Macro may be referenced in one or more System Operational Command Steps
10	Device Command Log	• Each Device Command Log entry is generated by one System Operation Command Schedule
11	Device Command Steps	• Each Device Command Step refers to one Device Command\ • Each Device Command Step refers to one Device Command Macro
12	Device Rules	• Each Device Rule references one Device
13	Device Status	• Each Device Status may describe one or more Devices.
14	Diagnostic Command	• Each Diagnostic Command has no associations or relationships with any other entity.
15	Emergency Notification Profile	• Each Emergency Notification Profile may describe one or more Personnel
16	Location	• Each Location may describe one or more Devices
17	Operator Daily Diary Log	• Each Operator Daily Diary Log entry is for one Personnel • Each Operator Daily Diary Log entry references one Workstation
18	Personnel	• Each Personnel has one Personnel Security Level • Each Personnel has one Personnel Status • Each Personnel has one Emergency Notification Profile • Each Personnel has one Personnel Classification • Each Personnel may be referenced in one or more Operator Daily Diary

#	Entity Name	Relationships
		Log entries • Each Personnel may be referenced in one or more System Operation Command Logs • Each Personnel may be referenced in one ore more Device Command Logs • Each Personnel may be referenced in one or more Problem Work Order Personnel
19	Personnel Classification	• Each Personnel Classification may describe one or more Personnel
20	Personnel Security Level	• Each Personnel Security Level may describe one or more Personnel • Each Personnel Security Level may be authorized for one or more Personnel Workstations • Each Personnel Security Level may be referenced by one or more Personnel Security Level Devices. • Each Personnel Security Level may be authorized for one or more Personnel System Functions • Each Personnel Security Level may be authorized for one or more Personnel System Modes • Each Personnel Security Level has one Command Level
21	Personnel Security Level Device	• Each Personnel Security Level Device references one Device and one Personnel Security Level
22	Personnel Status	• Each Personnel Status may describe one or more Personnel
23	Personnel System Functions	• Each Personnel System Function references one Personnel Security Level and one System Function
24	Personnel System Modes	• Each Personnel System Mode references one Personnel Security Level and one System Mode
25	Personnel Workstations	• Each Personnel Workstation references one Personnel Security Level
26	Problem Work Order	• Each Problem Work Order has one Problem Work Order Type • Each Problem Work Order has one Problem Work Order Status • Each Problem Work is referenced by one ore more Problem Work Order Personnel
27	Problem Work Order Personnel	• Each Problem Work Order Personnel associates all the Personnel associated with one Problem Work Order • Each Problem Work Order Personnel associates all the Problem Work Orders associated with one Personnel
28	Problem Work Order Status	• Each Problem Work Order Status may describe one or more Problem Work Orders
29	Problem Work Order Type	• Each Problem Work Order Type may describe one or more Problem Work Orders
30	Report Parameters	• Each Report Parameter has no associations or relationships with any other entity
31	Sign Message	• Each Sign Message has no associations or relationships with any other entity.
32	System Control Parameters	• Each System Control Parameter has no associations or relationships with any other entity
33	System Functions	• Each System Function may be referenced by one or more Personnel System Functions
34	System Mode	• Each System Mode may be used for one or more System Operation Schedules • Each System Mode may be referenced by one or more Personnel

#	Entity Name	Relationships
		System Modes
35	System Operation Command Log	• Each System Operation Command Log entry is generated by one System Operation Command Schedule execution • Each System Operation Command Log entry references one Personnel
36	System Operation Command Schedule	• Each System Operation Command Schedule item refers to one Agency • Each System Operation Command Schedule item refers to one System Mode • Each System Operation Command Schedule item creates one or more System Operation Command Log entries • Each System Operation Command Schedule item creates one or more Device Command Log entries • Each System Operation Command Schedule references one System Operational Command or Device Command Macro or Device Command. •
37	System Operation Status	• Each System Operation Status may be associated with one or more System Operation Command Log entries
38	System Operational Command Steps	• Each System Operational Command Step associates one Device Command Macro with all its System Operational Commands • Each System Operational Command Step associates one System Operational Command with all its Device Command Macros.
39	System Operational Command (Super Macro)	• Each System Operational Command (Super Macro) is composed of one or more System Operational Command Steps • Each System Operational Command may be referenced by one or more System Operation Command Schedules
40	Workstations	• Each Workstation may be referenced by one or more Operator Daily Diary Log entries. • Each Workstation may be referenced by one or more Personnel Workstations.

Appendix D – Hardware Interface I/O Card Pin Configuration

FCU – NORTH EXISTING HARDWARE INTERFACE

EXISTING INTERFACE CARD	SIGNAL VOLTAGE	SIGNAL TYPE	FIELD DEVICE/SENSOR
VME600	TXD A	RS 232 to Leased line modem	TSU
	RXD A		
	RTS A		
	CTS A		
	GND A		
	TXD B	RS 232 to Dial up modem	
	RXD B		
	GND B		
VME400	TXD	Serial Input / Output	DCU 4
	RXD		
	RTS		
	-		
	CTS		
	SIG. GND		
	DCD		
	-		
	TXD	Serial Input / Output	DCU 5
	RXD		
	RTS		
	-		
	CTS		
	SIG. GND		
	DCD		
	-		
VME400	TXD	Serial Input / Output	CMS 9
	RXD		
	RTS		
	-		
	CTS		
	SIG. GND		
	DCD		
	-		
	TXD	Serial Input / Output	CMS 10
	RXD		
	RTS		
	-		
	CTS		
	SIG. GND		
	DCD		

FCU – NORTH EXISTING HARDWARE INTERFACE

	-		
	TXD	Serial Input / Output to line drivers	CMS 11
	RXD		
	RTS		
	-		
	CTS		
	SIG. GND		
	DCD		
	-		
	TXD RXD	Serial Input / Output	CMS 12
	RTS		
	-		
	CTS		
	SIG. GND		
	DCD		
	-		
VME 200	24VDC	Digital Input / Output	Fire Alarm
			Watchdog status
			Yard gate B sensor
			Yard gate A sensor
			Equip. room sensor
			Controller sensor
			LHS light
			LHN light
			Air dryer sensor
			Air cooler sensor
			Air compressor monitor
			Air compressor power
			Back-up AC power sensor
			AC power monitor
	TBD	Digital Input / Output	Cab. ID 1's bit
	TBD		Cab. ID 2's bit
	TBD		Cab. ID 4's bit
	TBD		Cab. ID 8's bit
	TBD		Watchdog timer
	TBD		Reset I/P jack
	TBD		LHS lights
	TBD		LHN lights
VME 500	24VDC	Analog Input	Air tank +voltage
			Air tank GND voltage
			Air compressor +voltage
			Air tank +voltage
			Cable shield

FCU – SOUTH EXISTING HARDWARE INTERFACE

EXISTING INTERFACE CARD	SIGNAL VOLTAGE	SIGNAL TYPE	FIELD DEVICE/SENSOR
VME 600	TXD A	RS 232 to Leased line modem	TSU
	RXD A		
	RTS A		
	CTS A		
	GND A		
	TXD B	RS 232 to Dial up modem	
	RXD B		
	GND B		
VME 400	TXD	4-Wire Serial Input / Output	CMS 1
	RXD		
	RTS		
	CTS		
	SIG. GND		
	DCD		
VME 400	TXD	4-Wire Serial Input / Output	CMS 2
	RXD		
	RTS		
	CTS		
	SIG. GND		
	DCD		
VME 400	TXD	4-Wire Serial Input / Output	CMS 3
	RXD		
	RTS		
	CTS		
	SIG. GND		
	DCD		
VME 400	TXD	4-Wire Serial Input / Output	CMS 4
	RXD		
	RTS		
	CTS		
	SIG. GND		
	DCD		
VME 400	TXD	4-Wire Serial Input / Output	CMS 5
	RXD		
	RTS		
	CTS		
	SIG. GND		
	DCD		
VME 400	TXD	4-Wire Serial Input / Output	CMS 6
	RXD		
	RTS		
	CTS		
	SIG. GND		
	DCD		
VME 400	TXD	4-Wire Serial Input / Output	CMS 7
	RXD		

FCU – SOUTH EXISTING HARDWARE INTERFACE

	RTS		
	CTS		
	SIG. GND		
	DCD		
VME 400	TXD	4-Wire Serial Input / Output	CMS 8
	RXD		
	RTS		
	CTS		
	SIG. GND		
	DCD		
VME 400	TXD	4-Wire Serial Input / Output	DCU1
	RXD		
	RTS		
	CTS		
	SIG. GND		
	DCD		
VME 400	TXD	4-Wire Serial Input / Output	DCU2
	RXD		
	RTS		
	CTS		
	SIG. GND		
	DCD		
VME 400	TXD	4-Wire Serial Input / Output	DCU3
	RXD		
	RTS		
	CTS		
	SIG. GND		
	DCD		
VME 200	24VDC	Digital Input / Output	Fire Alarm
			Watchdog status
			Yard gate sensor
			Equip. room sensor
			Control room sensor
			LHS light
			LHN light
			Air dryer sensor
			Air cooler sensor
			Air compressor monitor
			Air compressor power
			Back-up AC power sensor
			AC power monitor
VME 200	TBD	Digital Input / Output	Cab. ID 1's bit
	TBD		Cab. ID 2's bit
	TBD		Cab. ID 4's bit
	TBD		Cab. ID 8's bit
	TBD		Watchdog timer
	TBD		Reset I/P jack
	TBD		LHS lights
	TBD		LHN lights
VME 500	24VDC	Analog Input	Air tank +voltage
			Air tank GND voltage
			Air compressor +voltage
			Air tank +voltage
			Cable shield

Appendix E – Transportation Electrical Equipment Specification (TEES) for the 2070 Controller

This document can be found at the Department of Transportation web site at

http://www.dot.ca.gov/hq/traffops/elecsys/2070/2070a.htm

Appendix F – Initial System Configuration Data for Operational Sequences and System Modes

This section describes the RLCS operational requirements which are critical to designing a safe control system. This section also lays down operational rules, which the software must implement and adhere to.

F.1 Open Entrances

RLCS facility entrances allow vehicles to enter from the adjacent main lanes of I-15 or SR-163. Each entrance serves only one direction of travel (either Northbound, or Southbound). Each entrance is, as necessary, opened in order to allow access to the facility, or closed in order to either close the facility, or open it in the opposing direction.

RLCS facility exits, used by vehicles to exit the facility, are always open and have no control devices associated with them.

In the direction of travel on the freeway, RLCS facility entrance closure devices consist of:

1. Changeable Message Signs (CMS)
2. Entrance Longitudinal Pop-ups
3. Entrance Transverse Pop-ups
4. Barrier Gates
5. Wrong Way Transverse Pop-ups
6. Wrong Way Longitudinal Pop-ups

Operation of each closure device will entail one or more commands from its associated control unit. Each command, which operates a single closure device, shall have a specific 'response time window' defined for successful command completion. In addition, each compound command, which includes more than one 'single device' command, shall have a specific 'response time window' defined for successful command completion of the compound command.

The control system must not attempt to open any entrance closure device, if the status of any opposite direction entrance closure device is 'unknown' or open'.

Steps within a command, or command group, shall be executed sequentially, whether the individual commands in a group, will be executed by one (1) control unit, or by more than one control unit.

F.2 Roadway Closure Device Status

The current status of all entrance closure devices in the system must be maintained at each control unit. The state of the closure devices shall be updated in all control units. The update frequency shall be higher during the opening and closing periods. Closure device sensors shall be monitored continuously by their local control unit. The status should be forwarded immediately to all other control units in the system.

F.3 Opening Sequences

Opening sequences must open Entrance devices in the following order:

1. Barrier Gate

2. Wrong Way Transverse Pop-ups
   If more than one bank, banks are opened in the direction from the freeway toward the reversible lanes.
3. Wrong Way Longitudinal Pop-ups
   Pop-up banks are opened beginning at the entrance ramp nose at the reversible lanes, and proceeding toward the edge of shoulder.
4. Entrance Transverse Pop-ups
   If more than one bank, the banks are opened in the direction from the reversible lanes toward the freeway.
5. Entrance Longitudinal Pop-ups
   Pop-up banks are opened downstream (entrance ramp nose at the freeway) to upstream (edge of shoulder).
6. CMS
   CMS messages will be changed from a 'Closed' message, to an 'Open' message beginning with the furthest downstream sign (sign closest to the reversible lane), and proceeding upstream (away from the reversible lanes) as message change confirmations are received from each sign.

At any point in an opening sequence, the sequence shall be halted if:

- A device fails to report completion of the current sequence step within the response time window allotted for the step, or
- The status of a closure device for the opposite direction of travel changes to 'unknown' or 'open', or
- The status of a closure device, which was previously opened at the current entrance, changes to 'unknown' or 'closed'.

F.4 Closing Sequences

Closing sequences must close Entrance devices in the following order:

1. CMS
   CMS messages will be changed from "Open" to "Closed" beginning with the farthest upstream sign (furthest away from the entrance) and proceeding, in order, downstream (towards the entrance). The system shall provide for a specific delay between the message change on each sign and the message change on the next downstream sign. The delay for each sign pair shall equal the time to travel between the two signs at a system specified speed.
2. Entrance Longitudinal Pop-ups
   Entrance Longitudinal Pop-ups must be closed in the direction of adjacent freeway traffic (beginning at the shoulder edge and proceeding toward the entrance ramp nose).
3. Entrance Transverse Pop-ups
   If more than one bank, Entrance Transverse Pop-ups will be closed in the direction from the freeway toward the reversible lanes.
4. Wrong Way Longitudinal Pop-ups
   Wrong Way Longitudinal Pop-ups will be closed beginning at the shoulder edge, and progressing toward the ramp nose, next to the reversible lanes.
5. Wrong Way Transverse Pop-ups
   If more than one bank, Wrong Way Transverse Pop-ups will be closed in the direction from the reversible lanes toward the freeway.

6. Barrier Gate

At any point in a closing sequence, the sequence shall be halted if either:

1. A device fails to report completion of the current sequence step within the response time window allotted for the step, or
2. The status for a closure device, which was previously closed at the current entrance, changes to 'unknown' or 'open'.

F.5 'Halted' Opening and Closing Sequences

A 'halted' opening or closing sequence shall cause the system to enter a 'hold' state for a system specified time. If the offending device status can be corrected within the specified time period, the operator shall be able to enter a 'resume' command in order for the system to attempt to complete the original opening/closing sequence.

F.6 Multiple Entrances

If multiple entrances exist on the reversible lanes in the direction of travel being opened, the specific order in which those entrances are opened presents no 'wrong way' safety issues. Likewise, if multiple entrances exist on the reversible lanes in the direction of travel being closed, the specific order in which those entrances are closed presents no 'wrong way' safety issues.

F.7 Safety Screening of Commands

Safety screening shall be done to determine if execution of a proposed command, if successful, would produce a valid reversible lanes configuration. If the screened command, including any subordinate commands would result in an unacceptable reversible lanes configuration, the screening check is considered to have failed.

In the following section, the term 'device command' shall be understood to include any simple command, command group, or macro, which may, if executed, change the state of one or more entrance devices.

In the case of device command groups (macros, compound commands, etc.) any screening requirement shall be applied to the command group, and to each device command within the group, prior to execution.

Each instance of safety screening shall utilize system configuration data that is no more than 3 seconds old.

Safety screening of device commands shall be multi-layered.

1. Safety screening shall be applied to all device commands at the originating control unit, and at all subordinate control units to which the device command or any of its subordinate device commands may be forwarded.
2. Safety screening shall always be applied to any device command, or command step, by any control unit which directly operates the target entrance closure device(s), <u>just prior to actual command execution</u>.

An opening or closing sequence shall be halted, with an appropriate error response to the system operator, if, at any sequence step, command safety screening fails.

F.8 Control System Integrity

Control Unit Non-Volatile Memory
In each FCU and DCU in the system, the following items shall be replicated from the central database server and maintained in non-volatile, non-removable memory:

Login Tables
Closure Device Timing Parameters
Air Calibration Factors
Reversible Lanes Configuration Table(s)
Reversible Lanes Operating Logic, Control Sequences, and Rule Sets

F.9 Control System Integrity Verification

The system shall will employ a one-way hash function as an aid to encrypting and maintaining the integrity of the data and software in the field. The hash value returned by the function shall will be at least 128 bits in length. The MD5 algorithm is acceptable for this purpose. This algorithm shall reside in all the controllers and the application server.

At each time, one or more of the above item types, listed under 'Control Unit Non-Volatile Memory', is created or modified, a UTC date/time stamp shall will be appended to the code (or table). The appending of the time stamp shall will be the last step in the process which builds the time stamped code/data section.

The system shall will also, for each control unit in the system, produce a table of the returned 'one-way hash function' (Message Digest) values, of each of the 'Control Unit Non-Volatile Memory' items. The returned 'Message Digest' values shall will be stored as hexadecimal characters. The appropriate 'Message Digest' table shall will be maintained in non-volatile memory in each system control unit.

The system will provide for periodic verification that current, recomputed 'Message Digest' values, for each unit in the system, correspond with 'record' values computed by the development process. The periodic evaluation shall will occur at least once a day. The 'Message Digest' value verification results shall will be recorded in the system log. A verification failure shall will cause an alarm condition for the affected control unit. If the failure occurs in checking the non-volatile memory items, the system shall will prevent the affected unit from being used in control sequences.

The system shall will provide for 'Message Digest' verification requests for a given unit by operator command.

For system login purposes, the hash function shall will also be used to encrypt user passwords.

The system will provide for password aging. Whether or not the system will require password aging shall will be controllable by the System Administrator.

The system will provide for minimum username and password lengths. The minimum length values shall will be controllable by the system administrator.

F.10 Access and Safety Characteristics of the I-15 Reversible Roadway

The software must implement.

Characteristics Bearing on Security

1. Isolation –
   System commands may be entered only at a control unit console following logon. Command pathways are hard-wired, and not shared with other devices or systems. The current state of the roadway may be transmitted from the upper control unit (TSU) to another system via a one-way serial link. The Reversible Lane Control System does not accept or process any input from other systems.

2. Closure Device Status Circulation –

   The current state of each roadway closure device and device status change is circulated to all control units in the system, every 2 seconds.

3. Command Forwarding –
   Commands are only forwarded from superior units to inferior units. This prevents a lower level unit from changing the state of a device which is controlled by either a higher level unit, or by a peer unit.
4. Command Processing –
   Device control units utilize device feedback, coupled with strict response time windows for device opening and closing commands.
5. Uncertain status –
   Unknown, or improper closure device status anywhere in the system, will immediately terminate a 'device opening' command. Improper device status 'may' terminate a device closing command, or sequence.

Physical Access/Control Table

Access Point	Control Ability
TMC	All RLCS Closure Devices
FCU South	All RLCS Closure Devices
DCU 1	NB 15 Entrance Wrong Way Devices and Gate
DCU 2	NB 163 Entrance Devices and Gate
DCU 3	NB 163 Wrong Way Devices
FCU North	All RLCS Closure Devices
DCU 4	SB 15 Wrong Way Devices
DCU 5	SB 15 Entrance Devices and Gate
CMS 1-12	Individual CMS Control

F.11 Normal Operations (Operator is logged on)

The system must allow the following scheduled operations at a minimum during 'normal' operational mode:

Sequence #1: Goal State: Open South Bound (AM) / Initial State: Closed (PM)
AM Opening South Bound at 5:20 AM. (Initially Gate 5 at Loc. 5 is OPEN)

Step #	Operation	Device	Location
	Status check by Operator	All	All
1	CLOSE	Gate 1	Loc. 1 South End 15
2	CLOSE	Gate 2	Loc. 2 South End 163
3	OPEN	WW-Pop-ups	Loc. 4
4	OPEN	Draw Light	North End 15
5	OPEN	EN-Pop-ups	Loc. 5
6	OPEN	CMS 9-12	North End 15

Sequence #2: Goal State: Closed (AM) / Initial State: Open South Bound (AM)
AM Closing South Bound at 11:00 AM

Step #	Operation	Device	Location
	Status check by Operator	All	All
1	CLOSE	CMS 9-12	North End 15
2	CLOSE	EN-Pop-ups	North End 15
3	CLOSE	WW-Pop-ups	North End 15
4	OPEN	Gate 1	Loc. 1 South End 15
5	OPEN	Gate 2	Loc. 2 South End 163

Sequence #3: Goal State: Open North Bound (PM) / Initial State: Closed (AM)
PM Opening North Bound at 11:15 AM

Step #	Status	Device	Location
	Status check by Operator	All	All
1	CLOSE	Gate 5	Loc. 5 North End 15
2	OPEN	WW Lights	Loc. 4 North End 15
3	OPEN	WW-Pop-ups	South End 163
4	OPEN	WW-Pop-ups	South End 15
5	OPEN	EN-Pop-ups	South End 15
6	OPEN	CMS 1-4	South End 15
7	OPEN	EN-Pop-ups	South End 163
8	OPEN	CMS 5-8	South End 163

Sequence #4: Goal State: Closed (PM) / Initial State: Open North Bound (PM)
PM Closing of RLCS at 7:00 PM.

Step #	Status	Device	Location
	Status check by Operator	All	All
1	CLOSE	CMS 1-4	South End 15
2	CLOSE	EN-Pop-ups	South End 15
3	CLOSE	WW-Pop-ups	South End 15
4	CLOSE	CMS 5-8	South End 163
5	CLOSE	EN-Pop-ups	South End 163
6	CLOSE	WW-Pop-ups	South End 163

7	CLOSE	WW-Lights	North End 15
8	OPEN	Gate 5	North End 15

F.12 Unattended Operations (No operator is logged on)

When no operator is logged on to the system, the status of all devices will continue to be monitored and displayed. If a scheduled operational sequence requires an operator to be logged on to confirm each step of the operation, an audible alarm will sound to alert the operator to log on to the system.

Appendix G – Requirements Working Group

Position	*Name*	*Company/Department*	
Stakeholder	Ross Cather	Department of Transportation – Chief of Traffic Special Studies	
Stakeholder	Lawrence Emerson	Department of Transportation – Traffic Operations	
Stakeholder	Harrison Makau	Department of Transportation – Software	
Stakeholder	Don Day	Department of Transportation Software	
Stakeholder	Dave Dutcher	Department of Transportation – Communications	
Stakeholder	Anupkumar Khant	Department of Transportation – Traffic Operations	
Stakeholder	Brian Pecus	Department of Transportation – Traffic Operations	
Stakeholder	David Pham	Department of Transportation – Software	
Consultant	Karen Thurston	VIP	
Consultant	Fred Wood	VIP	