

InnoVote ReliaVote Precinct Edition

Functional Design

By
Erin Thead
Software Engineer
erin@erinthead.com

© 2005

Table of Contents – ReliaVote Precinct Edition Functional Design

1.	Introduction.....	154
1.1.	Purpose.....	154
1.2.	Scope.....	154
1.3.	Definitions, Acronyms, and Abbreviations.	Error! Bookmark not defined.
1.4.	References.....	155
1.5.	Overview.....	155
2.	Overall Description.....	156
2.1.	Product Functions.	156
2.2.	User Classes.....	157
2.2.1.	Administrator user class.....	157
2.2.2.	System user	157
2.3.	Assumptions and Dependencies.	158
2.3.1.	Hardware platform assumption.....	158
2.3.2.	Internet connectivity assumption	158
2.3.3.	Single-user assumption	158
2.4.	Deployment of the Software.	159
3.	Specific Requirements	160
3.1.	Functional Requirements.....	160
3.1.1.	System Feature 1: Detect all equipment in the network	160
3.1.2.	System Feature 2: Login a user.....	161
3.1.3.	System Feature 3: Configure the Database.....	162
3.1.4.	System Feature 4: Program the SecureDRE machines	164
3.1.5.	System Feature 5: Accept real-time data from SecureDRE.....	165
3.1.6.	System Feature 6: Program the CardReader software	166
3.1.7.	System Feature 7: Program the CardReader ballot scanner.....	167
3.1.8.	System Feature 8: Accept real-time data from CardReader	168
3.1.9.	System Feature 9: Lock a SecureDRE-compatible machine	169
3.1.10.	System Feature 10: Unlock a SecureDRE-compatible machine.....	170
3.1.11.	System Feature 11: End election.....	171
3.1.12.	System Feature 12: Accept final data from SecureDRE.....	172
3.1.13.	System Feature 13: Accept final data from CardReader	173
3.1.14.	System Feature 14: Check voting results for anomalies	174
3.1.15.	System Feature 15: Accept error records from SecureDRE	175
3.1.16.	System Feature 16: Accept error records from CardReader	176
3.1.17.	System Feature 17: Detect central computer	177
3.1.18.	System Feature 18: Send results to a central computer	178
3.1.19.	System Feature 19: Display precinct election results	179
3.1.20.	System Feature 20: Detect and log errors	180
3.1.21.	System Feature 21: Accept and verify recount results.....	181
3.1.22.	System Feature 22: Display recount results.....	182
3.1.23.	System Feature 23: Clear election results	183

3.1.24.	System Feature 24: Clear election results from voting devices	184
3.1.25.	System Feature 25: View events.....	185
3.1.26.	System Feature 26: Create a new user	186
3.1.27.	System Feature 27: Change a user's password	187
3.1.28.	System Feature 28: Delete a user.....	188
3.1.29.	System Feature 29: Manually logout a user.....	189
3.1.30.	System Feature 30: Automatically logout a user	189
3.2.	Performance Requirements.....	190
3.2.1.	Performance Requirement 1: Modify Database quickly.....	190
3.2.2.	Performance Requirement 2: Transmit and receive data quickly	190
3.3.	Security Requirements.....	191
3.3.1.	Security Feature 1: Verify identity of data transmitters.....	191
3.3.2.	Security Feature 2: Encrypt Database tables	192
3.3.3.	Security Feature 3: Restrict data flow to Database tables.....	192
3.3.4.	Security Feature 4: Limit changes to Database on Election Day.....	193
3.3.5.	Security Feature 5: Virtual private network.....	193
3.3.6.	Security Feature 6: Encrypt outbound data.....	194
3.3.7.	Security Feature 7: Database login	194
3.3.8.	Security Feature 8: Block all ports except three	194
3.4.	System Attributes.....	195
3.4.1.	Reliability.....	195
3.4.2.	Availability	195
3.4.3.	Security	195
3.4.4.	Maintainability.....	195
3.4.5.	Portability.....	195
4.	Appendices.....	196

1. Introduction

1.1. Purpose.

The purpose of this document is to communicate the software requirements and functional design for the InnoVote ReliaVote Precinct Edition software. The document provides a detailed description of functional, performance, and security requirements, design constraints, and classes of persons who will be using the software.

The intended audience of this document is the developer and any other persons interested in the project, including election reform activists, computer security professionals, political figures with an interest in election reform, and potential buyers of the design.

1.2. Scope.

InnoVote ReliaVote Precinct Edition (PE) is one component of an interoperable line of products. It is a software product designed to execute on a standard commercially available Intel™ or Macintosh™-compatible computer.

ReliaVote PE will send and receive input from any voting equipment executing InnoVote SecureDRE [ref. 7] and InnoVote CardReader [refs. 1 and 2]. ReliaVote PE will store election data received from these products in a secure electronic database for later transmission to a central tabulator.

ReliaVote PE will also have the ability to initiate certain operations on the SecureDRE and CardReader software by sending data transmissions to these products in a form that they will be able to recognize. The details of the operations that ReliaVote PE can initiate on external machines can be found in references [2] and [7].

Current vote tabulation software is insecure and unreliable. Existing tabulators, which are used in voting sites across the United States, have had numerous and severe documented errors and security problems, including the following:

- Little to no protection of vote tallies from tampering
- The suspicion of pre-election and pre-recount rigging of tabulators
- Unverified updates being made to election software
- Public online access to sensitive operations of election software

ReliaVote PE is a highly secure and accountable system with strong anti-fraud protection. Election data are heavily protected both from errors and from tampering. In the event that data stored on a ReliaVote PE machine *are* compromised, the system

will detect this and inform the users (presumably election officials) of it, at which point they can act in a manner prescribed by law with respect to ensuring the integrity of the data. As is described in references [2], [6], and [7], other InnoVote products have built-in security measures to ensure that at least one uncompromised copy of an election's data will remain.

1.3. References.

- [1] Thead, E. *InnoVote CardReader Hardware Requirements Overview*, 2005.
- [2] Thead, E. *InnoVote CardReader Functional Design*, 2005.
- [3] Thead, E. *InnoVote Database Detailed Design*, 2005.
- [4] Thead, E. *InnoVote MyVotronic Hardware and Operating System Overview*, 2005.
- [5] Thead, E. *InnoVote Network Detailed Design*, 2005.
- [6] Thead, E. *InnoVote ReliaVote Central Server Functional Design*, 2005.
- [7] Thead, E. *InnoVote SecureDRE Functional Design*, 2005.
- [8] Thead, E. *InnoVote Database Access Matrix*, 2005.
- [9] Thead, E. *Security Analysis of InnoVote Products*, 2005.

1.4. Overview.

The remainder of this document is organized in the following fashion:

Section 2: Provides overall description of the system, including product functions, user classes, assumptions, and generalized dependencies.

Section 3: Provides specific requirements including functional requirements, performance requirements, and security requirements.

Section 4: Provides supporting figures and tables for information in other sections of the document.

2. Overall Description

2.1. Product Functions.

ReliaVote Precinct Edition will need to perform the following basic functions:

1. Provide user authentication measures to ensure that no unauthorized persons may use the software
2. Provide user management features to add, modify, and remove software users
3. Detect all voting equipment in the precinct with which it will have to communicate
4. Detect the county's central computer with which it will communicate
5. Accept data transfers from the ReliaVote Central Server software product to "program" the machine, or, alternatively, allow a user to program it directly. This involves adding and/or modifying entries in Database tables.
6. Send data transfers to a SecureDRE-compatible DRE machine to "program" the machine.
7. Send data transfers to a CardReader-compatible ballot scanner to "program" the machine.
8. Accept real-time vote data from voting equipment in the network
9. Send a signal to all voting equipment in the precinct to indicate that the election is ended
10. Lock input from and output to hardware when an election is over
11. Unlock hardware to allow input and output
12. Receive final vote information and tallies from voting equipment
13. Check the finalized votes and tallies against each other and against the real-time votes, and disallow further transmission if there are anomalies
14. Send the final verified vote results and tallies the central PC
15. Display precinct-level election results
16. Accept, verify, and display recount results from CardReader
17. Maintain error logs for itself and receive error logs from voting equipment in the network

2.2. User Classes.

2.2.1. Administrator user class

The Administrator user class represents any person who has the legal authority to use a computer in the possession of a Board of Elections and view the results of an election. This class of user will need to initiate operations that modify sensitive tables in the InnoVote Database but should *not* have direct access to the Database.

Administrator privileges are granted to any user who has knowledge of a correct user name and password for ReliaVote PE.

An Administrator does not have direct access to the Database. Any requests for modifications to the database will be performed at the System privilege level.

2.2.2. System user

The System shall function as a user class. It must be able to perform any operation necessary on the hardware and data stored in the system, within the permission scheme of the computer's operating system. Operations in software functions initiated by Administrators may be executed at System level. These functions are described in §3 of this document.

The System will in theory have full access to the Database at all times, but the software must be coded so that it will in *practice* not perform certain damaging operations to the Database, and that no human user or external machine will be able to interact with ReliaVote PE with System privileges. Additionally, the Database shall be configured to disallow certain actions [reference 2].

2.3. Assumptions and Dependencies.

2.3.1. Hardware platform assumption

The document assumes that InnoVote ReliaVote PE will execute on an Intel- or Macintosh-compatible processor. It should exist in versions for at least the following operating system families: Microsoft® Windows®, Macintosh® OS X®, and Linux.

2.3.2. Internet connectivity assumption

The document assumes that hardware running InnoVote ReliaVote PE will be connected to a TCP/IP-compatible network during operation. IP version 6 is not necessary for correct operation of ReliaVote PE, but it does provide extra security benefits.

2.3.3. Single-user assumption

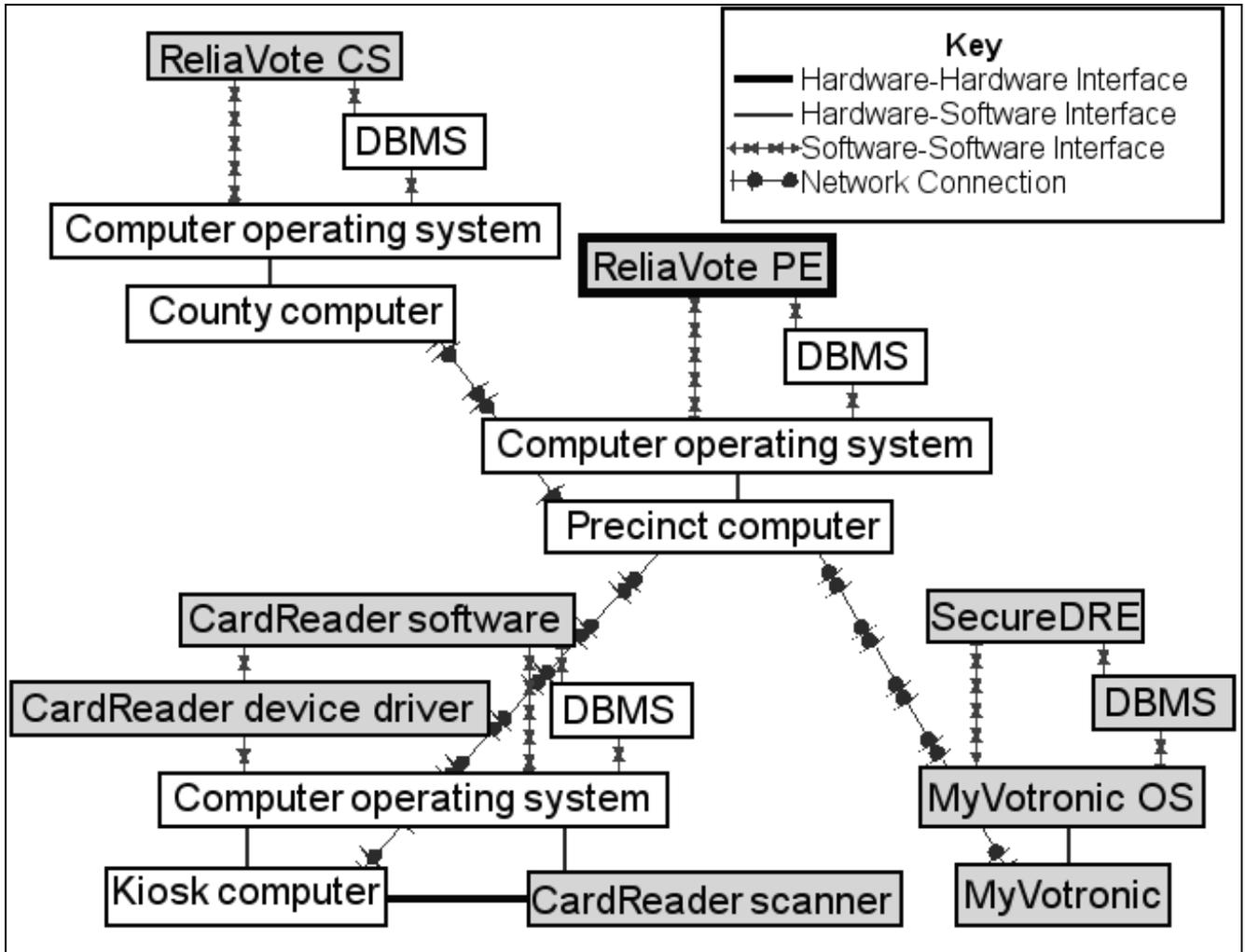
The document assumes that ReliaVote PE is a single-user software product. Although there is no provision for user profiles and logins, it is conceivable that ReliaVote PE could receive instructions from more than one concurrent source or “user,” as defined by the User Classes (§2.2) in this document.

For any set of operations that could potentially be in conflict, the operation currently being executed by the System user has precedence. Next are operations that were initiated by Administrators.

2.4. Deployment of the Software.

Figure 1 shows the deployment diagram for all InnoVote products and necessary third-party components. Items that this document describes are surrounded with thick boxes.

Figure 1: Deployment Diagram.



3. Specific Requirements

3.1. Functional Requirements.

The features described in this section are operations that are necessary for correct and useful operation of the ReliaVote PE software product.

3.1.1. System Feature 1: Detect all equipment in the network

3.1.1.1. Purpose of Feature

This feature allows the system to obtain a list of all equipment that is connected to the precinct computer over a private network. The system will also obtain detailed information about each device and store all the information it obtains. This feature will need to be able to immediately detect the following changes to the network configuration:

- Addition of a new device to the network
- Removal of a device from the network
- Any change to any device attribute for which ReliaVote PE is maintaining a record

3.1.1.2. Stimulus-Response Sequence

1. The system employs a stable network routing algorithm to determine what devices are connected to the network.
2. The system creates a unique network identification for each device.
3. The system records the IP address of each device.
4. The system sends a data transmission to each device requesting its type of equipment, its hardware version, its software version, and its current status.
5. The system receives a data transmission from each device containing the requested information.
6. The system stores the information it received.
7. The system records an entry in its Events table of the Database indicating the successful configuration of the network.

3.1.1.3. Dependencies

This operation requires the completion of no other System Features before it can begin execution.

This feature is restricted by Security Features 5, “Limit changes to Database on Election Day,” and 8, “Block all ports except one.” The operation requires Security Features 2, “Verify identity of data transmitters,” 3, “Encrypt Database tables,” 7, “Encrypt outbound data,” and 8, “Block all ports except three.”

3.1.2. System Feature 2: Login a user

3.1.2.1. Purpose of Feature

This feature allows the system to authenticate a stored username and grant the user privileges to perform the remainder of the system features.

3.1.2.2. Stimulus-Response Sequence

1. A user indicates to the system that he or she wishes to login.
2. The system prompts the user for a username.
3. The user inputs a username to the system.
4. The system validates the username against a list of usernames.
5. The operation of the system depends on the result of Step 4.
 - a. If the user's username is present on the system's list, the system executes Steps 6 – 9.
 - b. If the user's username is not present, the system displays an error message indicating that the username is not valid and reverts to Step 2.
6. The system prompts the user for a password.
7. The user inputs a password to the system.
8. The system validates the password against the password stored for the username that the user is attempting to use.
9. The operation of the system depends on the result of Step 8.
 - a. If the user's password matches the password that the system has stored, then the system executes Steps 10 – 11.
 - b. If the user's password is not correct, the system displays an error message indicating that the password is not valid and reverts to Step 6.
 - c. If the user inputs an incorrect password 5 consecutive times for a particular username, the system reverts to Step 2 and creates an entry in its Events Database table indicating that a user input an incorrect password 5 times. The entry also contains the username that the user was attempting to use and the date and time of each login attempt.
10. The system creates an entry in its Events table indicating that the username has logged in. This entry also contains the date and time of the login and the number of attempts that the user required to input the correct password.
11. The system displays the ReliaVote PE main screen to the user and grants the user Administrator privileges, and with this, the ability to perform the remainder of the System Features.

3.1.2.3. Dependencies

This operation requires the completion of no other System Features before it can begin execution. Conditional: If a user is already logged in, then that user must logout before a new user can login. ReliaVote PE is not a multi-user software product.

3.1.3. System Feature 3: Configure the Database

3.1.3.1. Purpose of Feature

This feature allows an authenticated user to store in the Database lists of election information, plus all contests, candidates/ballot options, and political parties that are participating in the election. Alternatively, the feature allows the system to accept programming from an authenticated ReliaVote CS computer.

It should be noted that either source of data (a user or ReliaVote CS) can overwrite programming written by the other.

3.1.3.2. Stimulus-Response Sequence

1. A user indicates to the system that he or she wishes to configure the Database.
2. The system displays an interface for the user to input the contests, candidates/ballot options, political parties, and any pertinent information about the data items. This interface allows the user to add, modify, and delete entries.
3. The system reads the item input by the user and the requested operation to perform on it.
4. The system attempts to perform the operation.
5. The system's operation depends on the result of Step 4.
 - a. If the operation is permitted by the database management system, the system executes it.
 - b. If the operation is not permitted, the system rejects it and displays a message to the user indicating the reason for its rejection.
6. The system reverts to Step 2 and continues the sequence of steps until the user indicates that he or she is finished.
7. The system reads the user's input indicating completion of the configuring.
8. The system records an entry in its Events Database table and displays the ReliaVote PE main screen to the user.

3.1.3.3. Alternate Stimulus-Response Sequence

1. The system receives a data transmission from the central computer containing Database configuration instructions and data. This transmission can contain requests to add, modify, and/or delete entries in Database tables.
2. The system attempts to perform the operations.
3. The system's operation depends on the result of Step 2.
 - a. If the operation is permitted by the database management system, the system executes it.
 - b. If the operation is not permitted, the system rejects it and logs an error message in its "Events" Database table.
4. The system sends an acknowledgment to the central computer detailing which transmissions were successfully performed and which were rejected.

3.1.3.4. Dependencies

Stimulus-Response Sequence 3.1.3.2 requires the successful completion of System Feature 2, “Login a user,” before it can begin execution.

Stimulus-Response Sequence 3.1.3.2. is restricted by Security Feature 4, “Limit changes to Database on Election Day.” The feature requires Security Feature 7, “Database login.”

Stimulus-Response Sequence 3.1.3.3 requires the successful completion of System Feature 16, “Detect central computer,” before it can begin execution.

Stimulus-Response Sequence 3.1.3.3. requires Security Features 1, “Verify identity of data transmitters,” and 6, “Encrypt outbound data.”

3.1.4. System Feature 4: Program the SecureDRE machines

3.1.4.1. Purpose of Feature

This feature allows the system to configure the Database of any SecureDRE-compatible voting machine over a network.

3.1.4.2. Stimulus-Response Sequence

1. The user indicates to the system that he/she wishes to program the database of one or more SecureDRE-compatible voting machines on the network.
2. The system displays a list of all SecureDRE-compatible voting machines that it has detected.
3. The user selects either a single machine or multiple machines to program.
4. The system creates a copy in RAM of the contests, candidates, and political parties that are stored in the Database tables.
5. The system sends the data to the selected SecureDRE-compatible voting machine or machines.
6. The system receives a notification from the machine(s) of the machine's success or failure to add the data.
7. The system's operation depends on the results of Step 6.
 - a. If the notification indicates a success, the system records an entry in its Events Database table and displays a message to the user that the data were successfully added to the machine.
 - b. If the notification indicates a failure, the system displays a message to the user that the programming failed. This message also contains the error code and error message sent by the voting machine.
8. The system displays the ReliaVote PE main screen.

3.1.4.3. Dependencies

This feature requires the successful completion of System Features 1, "Detect all equipment in network," and 3, "Configure the Database," before it can begin execution.

This feature is restricted by Security Feature 4, "Limit changes to Database on Election Day." It requires Security Features 1, "Verify identity of data transmitters," 6, "Encrypt outbound data," and 7, "Database login."

3.1.5. System Feature 5: Accept real-time data from SecureDRE

3.1.5.1. Purpose of Feature

This feature allows the system to accept and store real-time vote data transmissions from a SecureDRE-compatible system.

3.1.5.2. Stimulus-Response Sequence

1. The system receives a request from a SecureDRE-compatible voting machine to transmit real-time vote data.
2. The system sends a response to the voting machine asking for its real-time data.
3. The system receives the data from the voting machine.
4. The system attempts to add the data to the Database, authenticating itself to the Database.
5. The system's operation depends on the result of Step 4.
 - a. If the system successfully added the data to the Database, it transmits a response to the machine that the data were successfully added and executes Step 9.
 - b. If the system failed to add the data to the Database, it transmits a response to the machine that the data were rejected and executes Steps 6 – 9.
6. The system creates an entry in the "Events" table containing the error code, the machine on which the error occurred, the date and time of the error, and any other error information.
7. The system displays a message to the user that the data were rejected from the Database and gives the user the option of either dismissing the message or locking the voting machine on which the data originated. This message also contains any error codes and error messages generated by the database management system.
8. The system processes the user's input from Step 7. Conditional: If the user chose to lock the voting machine, the system executes System Feature 8, "Lock a SecureDRE-compatible machine."
9. The system records an entry in its Events Database table and displays the ReliaVote PE main screen.

3.1.5.3. Dependencies

This feature requires the successful completion of System Feature 4, "Program the SecureDRE Software," before it can begin execution.

This feature requires Security Features 1, "Verify identity of data transmitters," 2, "Encrypt Database tables," 6, "Encrypt outbound data," and 7, "Database login." It is restricted by Security Feature 3, "Restrict data flow to Database tables."

3.1.6. System Feature 6: Program the CardReader software

3.1.6.1. Purpose of Feature

This feature allows the system to configure the Database and ballot scanner of any CardReader-compatible ballot-scanning machine over a network.

3.1.6.2. Stimulus-Response Sequence

1. The user indicates to the system that he/she wishes to program the database of one or more CardReader-compatible ballot-scanning machines on the network.
2. The system displays a list of all CardReader-compatible ballot-scanning machines that it has detected.
3. The user selects either a single machine or multiple machines to program.
4. The system creates a copy in RAM of the contests, candidates, and political parties that are stored in the Database tables.
5. The system sends the data to the selected CardReader-compatible machine or machines.
6. The system receives a notification from the machine(s) of the machine's success or failure to add the data.
7. The system's operation depends on the results of Step 6.
 - a. If the notification indicates a success, the system displays a message to the user that the data were successfully added to the machine.
 - b. If the notification indicates a failure, the system displays a message to the user that the programming failed. This message also contains the error code and error message sent by the machine.
8. The system records a message in the Events Database table indicating the success or failure of the configuration.

3.1.6.3. Dependencies

This feature requires the successful completion of System Features 1, "Detect all equipment in network," and 3, "Configure the Database," before it can begin execution.

This feature is restricted by Security Feature 4, "Limit changes to Database on Election Day.". It requires Security Features 1, "Verify identity of data transmitters," 6, "Encrypt outbound data," and 7, "Database login."

3.1.7. System Feature 7: Program the CardReader ballot scanner

3.1.7.1. Purpose of Feature

This feature allows a user to map areas of a ballot rendering to specific ballot options that are stored in the Database and to transmit the configuration to one or more CardReader-compatible ballot-scanning machines in the network.

3.1.7.2. Stimulus-Response Sequence

1. The user indicates that he/she wishes to program the ballot scanner on the CardReader machine.
2. The system displays an electronic rendering of a sample ballot to the user.
3. The user indicates to the system which areas of the ballot are to be scanned for markings.
4. For each area of the ballot that the user selects, the system prompts the user to associate it with an entry in the “Running” Database table (a combination of a precinct, contest, and candidate).
5. The system maps the candidate-contest-precinct option to the user-selected ballot area, overwriting any existing mapping for the ballot area and ballot option.
6. The system repeats steps 4 and 5 until the user indicates that he/she has finished configuring the ballot scanner *and* all candidate/contest combinations in the Database for a particular precinct are mapped.
7. The system creates a copy in RAM of the configuration.
8. The system sends the data to the selected CardReader-compatible machine or machines.
9. The system receives a notification from the machine(s) of the machine’s success or failure to add the data.
10. The system’s operation depends on the results of Step 9.
 - a. If the notification indicates a success, the system logs a message in the “Events” database table indicating the configuration event and displays a message to the user that the machine was successfully configured.
 - b. If the notification indicates a failure, the system displays a message to the user that the programming failed. This message also contains the error code and error message sent by the voting machine. The system records an error message in the Events database table.
11. The system displays the ReliaVote PE main screen.

3.1.7.3. Dependencies

This feature requires the successful completion of System Feature 6, “Program the CardReader software,” before it can begin execution.

This feature is restricted by Security Feature 4, “Limit changes to Database on Election Day.” It requires Security Features 1, “Verify identity of data transmitters,” 6, “Encrypt outbound data,” and 7, “Database login.”

3.1.8. System Feature 8: Accept real-time data from CardReader

3.1.8.1. Purpose of Feature

This feature allows the system to accept and store real-time vote data transmissions from a CardReader system.

3.1.8.2. Stimulus-Response Sequence

1. The system receives a request from a CardReader-compatible ballot-scanning machine to transmit real-time vote data.
2. The system sends a response to the machine asking for its real-time data.
3. The system receives the data from the machine.
4. The system attempts to add the data to the Database.
5. The system's operation depends on the result of Step 4.
 - a. If the system successfully added the data to the Database, it records an entry in the Events Database table, transmits a response to the machine that the data were successfully added, and executes Step 9.
 - b. If the system failed to add the data to the Database, it transmits a response to the machine that the data were rejected and executes Steps 6 – 9.
6. The system creates an entry in the Events table containing the error code, the machine on which the error occurred, the date and time of the error, and any other error information.
7. The system displays a message to the user that the data were rejected from the Database and allows the user to dismiss the message. This message also contains any error codes and error messages generated by the database management system.
8. The system processes the user's input from Step 7.
9. The system displays the ReliaVote PE main screen.

3.1.8.3. Dependencies

This feature requires the successful completion of System Feature 7, "Program the CardReader ballot scanner," before it can begin execution.

This feature requires Security Features 1, "Verify identity of data transmitters," 2, "Encrypt Database tables," and 6, "Encrypt outbound data." It is restricted by Security Feature 3, "Restrict data flow to Database tables."

3.1.9. System Feature 9: Lock a SecureDRE-compatible machine

3.1.9.1. Purpose of Feature

This feature allows the system to instruct a MyVotronic or other SecureDRE-compatible DRE machine to prevent the machine from accepting further input from voters.

3.1.9.2. Stimulus-Response Sequence

1. The system transmits a data packet to a MyVotronic machine running SecureDRE-compatible software. The packet contains instructions to disable all hardware input and output except for the MyVotronic's network adapter.
2. The system receives a data transmission from the MyVotronic indicating that the voting machine has successfully locked its hardware.
3. The system records an entry in the Events Database table.

3.1.9.3. Dependencies

This feature requires the successful completion of System Feature 2, "Login a user," before it can begin execution.

This feature requires Security Features 1, "Verify identity of data transmitters," and 6, "Encrypt outbound data."

3.1.10. System Feature 10: Unlock a SecureDRE-compatible machine

3.1.10.1. Purpose of Feature

This feature allows the system to instruct a locked MyVotronic or other SecureDRE-compatible DRE machine to allow input from voters.

3.1.10.2. Stimulus-Response Sequence

1. The system transmits a data packet to a locked MyVotronic machine running SecureDRE-compatible software. The packet contains instructions to break the lock and allow input from and output to the MyVotronic's hardware.
2. The system receives a data transmission from the MyVotronic indicating that the voting machine has successfully unlocked its hardware.
3. The system records an entry in the Events database table.

3.1.10.3. Dependencies

This feature requires the successful completion of System Feature 9, "Lock a SecureDRE-compatible machine," before it can begin execution.

This feature requires Security Features 1, "Verify identity of data transmitters," and 6, "Encrypt outbound data."

3.1.11. System Feature 11: End election

3.1.11.1. Purpose of Feature

This feature allows the system to end an election and send data transmissions to all voting devices in the network instructing the machines to disallow input. It also blocks the ReliaVote PE software from accepting any input from the machines after the data transmission has been sent.

3.1.11.2. Stimulus-Response Sequence

1. The user indicates to the system that he/she wishes to declare the election over for the precinct.
2. The system checks its internal time against the poll-closing time attribute in the “Elections” table in the Database.
3. The system’s operation depends on the result of Step 2.
 - a. If the internal time is earlier than the poll-closing time, the system disallows the operation and records an error in the Events Database table.
 - b. If the internal time is later than the poll-closing time, the system performs System Feature “Lock a SecureDRE-compatible machine” for every SecureDRE-compatible voting machine present in the network. It records an entry in the Events Database table.

3.1.11.3. Dependencies

This feature requires the completion of no System Features to begin execution. This feature requires Security Features 1, “Verify identity of data transmitters,” 6, “Encrypt outbound data,” and 7, “Database login.” It is restricted by Security Feature 4, “Limit changes to Database on Election Day.”

3.1.12. System Feature 12: Accept final data from SecureDRE

3.1.12.1. Purpose of Feature

This feature allows ReliaVote PE to accept and store the final election results from each SecureDRE-compatible voting machine in the network.

3.1.12.2. Stimulus-Response Sequence

1. The system receives a request from a SecureDRE-compatible voting machine to send its finalized vote tallies and “Votes” Database table.
2. The system sends a response to the machine requesting its final tallies and votes.
3. The system receives the data from the machine.
4. The system attempts to add the data to the Database.
5. The system’s operation depends on the result of Step 4.
 - a. If the system successfully added the data to the Database, it transmits a response to the machine that the data were successfully added, generates an entry in the Events Database table, and executes Step 9.
 - b. If the system failed to add the data to the Database, it transmits a response to the machine that the data were rejected and executes Steps 6 – 9.
6. The system creates an entry in the Events table containing the error code, the machine on which the error occurred, the date and time of the error, and any other error information.
7. The system displays a message to the user that the data were rejected from the Database and allows the user to dismiss the message. This message also contains any error codes and error messages generated by the database management system.
8. The system processes the user’s input from Step 7.
9. The system displays the ReliaVote PE main screen.

3.1.12.3. Dependencies

This feature requires the successful completion of System Feature 11, “End election.”

This feature requires Security Features 1, “Verify identity of data transmitters,” 2, “Encrypt Database tables,” 6, “Encrypt outbound data,” and 7, “Database login.” It is restricted by Security Feature 3, “Restrict data flow to Database tables.”

3.1.13. System Feature 13: Accept final data from CardReader

3.1.13.1. Purpose of Feature

This feature allows ReliaVote PE to accept and store the final election results from each CardReader-compatible ballot-scanning machine in the network.

3.1.13.2. Stimulus-Response Sequence

1. The system receives a request from a CardReader-compatible ballot-scanning machine to send its finalized vote tallies and “Votes” Database table.
2. The system sends a response to the machine requesting its final tallies and votes.
3. The system receives the data from the machine.
4. The system attempts to add the data to the Database.
5. The system’s operation depends on the result of Step 4.
 - a. If the system successfully added the data to the Database, it transmits a response to the machine that the data were successfully added, records an entry in the Events Database table, and executes Step 9.
 - b. If the system failed to add the data to the Database, it transmits a response to the machine that the data were rejected and executes Steps 6 – 9.
6. The system creates an error entry in the Events table containing the error code, the machine on which the error occurred, the date and time of the error, and any other error information.
7. The system displays a message to the user that the data were rejected from the Database and allows the user to dismiss the message. This message also contains any error codes and error messages generated by the database management system.
8. The system processes the user’s input from Step 7.
9. The system displays the ReliaVote PE main screen.

3.1.13.3. Dependencies

This feature requires the successful completion of System Feature 11, “End election.”

This feature requires Security Features 1, “Verify identity of data transmitters,” 2, “Encrypt Database tables,” 6, “Encrypt outbound data,” and 7, “Database login.” It is restricted by Security Feature 3, “Restrict data flow to Database tables.”

3.1.14. System Feature 14: Check voting results for anomalies

3.1.14.1. Purpose of Feature

This feature allows ReliaVote PE to check three sources of election data – real-time voting results, finalized votes, and final candidate tallies – for inconsistencies and anomalies. It prevents the further transmission of inconsistent data.

3.1.14.2. Stimulus-Response Sequence

1. The system creates copies in RAM of the Database tables containing ballots, real-time individual votes, final individual votes, and final candidate tallies.
2. The system parses the real-time vote table and calculates candidate tallies from the entries in the table. It excludes any votes from the tallies if they are associated with an archived ballot.
3. The system parses the final vote table and calculates candidate tallies from the entries in the table. It excludes any votes from the tallies if they are associated with an archived ballot.
4. The system compares the two calculated candidate tallies to the separately stored candidate tallies and to each other.
5. The system's behavior depends on the result of Step 4.
 - a. If all three tallies are the same for every candidate on the ballot, then the system records a success entry in the Events, performs System Feature 18, "Send results to a central computer," and exits this sequence of steps.
 - b. If any one of the three tallies for any candidate is different from the other two, then the system performs Steps 6 – 9.
6. The system displays a prominent message to the user indicating that the vote totals do not all match and recommends a recount of the paper ballots.
7. The system blocks transmission of its vote data to the central computer.
8. The system generates entries in the Events table in the Database detailing what has occurred.
9. The system transmits a message to the central computer indicating that it has encountered a tallying discrepancy. This message also contains a unique identifier for the precinct or voting site.

3.1.14.3. Dependencies

This feature requires the successful completion of one of the following:

- a. System Features 15, "Accept final data from SecureDRE," and 5, "Accept real-time data from SecureDRE"
- b. System Features 16, "Accept final data from CardReader," and 18, "Accept real-time data from CardReader"
- c. Both (a) and (b), if the network contains both SecureDRE- and CardReader-compatible machines

This feature requires Security Features 1, "Verify identity of data transmitters," 2, "Encrypt Database tables," 6, "Encrypt outbound data," and 7, "Database login." It is restricted by Security Feature 3, "Restrict data flow to Database tables."

3.1.15. System Feature 15: Accept error records from SecureDRE

3.1.15.1. Purpose of Feature

This feature allows the ReliaVote PE system to accept and store error records from all SecureDRE-compatible voting machines in the network.

3.1.15.2. Stimulus-Response Sequence

1. The system receives a request from a SecureDRE-compatible voting machine to send an error record from its “Events” Database table.
2. The system sends a response to the machine requesting its error record.
3. The system receives the data from the machine.
4. The system attempts to add the record to its Events table in the Database.
5. The system’s operation depends on the result of Step 4.
 - a. If the system successfully added the data to the Database, it transmits a response to the machine that the data were successfully added and executes Step 9.
 - b. If the system failed to add the data to the Database, it transmits a response to the machine that the data were rejected and executes Steps 6 – 9.
6. The system creates an entry in the Events table containing the error code, the machine on which the error occurred, the date and time of the error, and any other error information.
7. The system displays a message to the user that the data were rejected from the Database and allows the user to dismiss the message. This message also contains any error codes and error messages generated by the database management system.
8. The system processes the user’s input from Step 7.
9. The system displays the ReliaVote PE main screen.

3.1.15.3. Dependencies

This feature requires the successful completion of System Feature 4, “Program the SecureDRE software.”

This feature requires Security Features 1, “Verify identity of data transmitters,” 6, “Encrypt outbound data,” and 7, “Database login”.

3.1.16. System Feature 16: Accept error records from CardReader

3.1.16.1. Purpose of Feature

This feature allows the ReliaVote PE system to accept and store error records from all CardReader-compatible ballot readers in the network.

3.1.16.2. Stimulus-Response Sequence

1. The system receives a request from a CardReader-compatible ballot-scanning machine to send an error record from its “Events” Database table.
2. The system sends a response to the machine requesting its error record.
3. The system receives the data from the machine.
4. The system attempts to add the record to its Events table in the Database.
5. The system’s operation depends on the result of Step 4.
 - a. If the system successfully added the data to the Database, it transmits a response to the machine that the data were successfully added and executes Step 9.
 - b. If the system failed to add the data to the Database, it transmits a response to the machine that the data were rejected and executes Steps 6 – 9.
6. The system creates an entry in the Events table containing the error code, the machine on which the error occurred, the date and time of the error, and any other error information.
7. The system displays a message to the user that the data were rejected from the Database and allows the user to dismiss the message. This message also contains any error codes and error messages generated by the database management system.
8. The system processes the user’s input from Step 7.
9. The system displays the ReliaVote PE main screen.

3.1.16.3. Dependencies

This feature requires the successful completion of System Feature 7, “Program the CardReader ballot scanner.”

This feature requires Security Features 1, “Verify identity of data transmitters,” 6, “Encrypt outbound data,” and 7, “Database login.”

3.1.17. System Feature 17: Detect central computer

3.1.17.1. Purpose of Feature

This feature allows the precinct computer to establish a means of communication with the county's central computer, which is running InnoVote ReliaVote CS or compatible software.

3.1.17.2. Stimulus-Response Sequence

1. The system obtains the IP address of the central computer and the port number on which the ReliaVote Central Server software is listening for connections from ReliaVote PE-compatible systems within the county. (The system can obtain this information either from a stored list or from user input.)
2. The system accesses the county's Kerberos server and receives a ticket for the county server.
3. The system sends a "beacon" packet to the machine at the IP address and port number that it has read. The packet contains instructions to send back a particular response.
4. The behavior of the system depends on the success of Step 3.
 - a. If the IP address does not exist or the port number is not open, the system does not receive any packet in response. It displays an error message after a given period of time and records the event in the Events table of the Database. It then exits this series of steps.
 - b. If the packet was received but could not be decrypted, the recipient sends back a generic acknowledgment packet. The system executes Steps 5 – 7.
 - c. If the packet was received and decrypted, the recipient sends back the correct data. The system stores the IP address and port number as the correct address and port number for communication with the central computer and records a success event in the Events table. It then exits this series of steps.
5. The system processes the packet and determines that the machine it sent its packet to was not the central computer.
6. The system outputs an error message to the user and records the event in the Events table of the Database.
7. The system reverts to Step 1.

3.1.17.3. Dependencies

This feature requires the successful completion of System Feature 2, "Login a user," before it can begin execution.

This feature requires Security Features 1, "Verify identity of data transmitters," 6, "Encrypt outbound data," and 7, "Database login."

3.1.18. System Feature 18: Send results to a central computer

3.1.18.1. Purpose of Feature

This feature allows the system to transmit the final candidate tallies, individual vote Database entries, and error records to a central tabulation server. This step can be performed on initial or recounted results, depending on the state of the system.

3.1.18.2. Stimulus-Response Sequence

1. The system determines whether it is in “Recount Mode.”
2. The system creates a plain-text copy in RAM of the “Votes” or (if it is in Recount Mode) “Recount_Votes” Database table.
3. The system creates a plain-text copy in RAM of the “Tallies” or (if it is in Recount Mode) “Recount_Tallies” Database table.
4. The system creates a plain-text copy in RAM of the “Events” Database table.
5. The system transmits the copies created in Steps 1 – 3 to the central computer.
6. The system receives an acknowledgment from the precinct computer containing the precinct computer’s success or failure to add the data to its own database. Conditional: If the system receives notification of a failure, it reverts to Step 4.
7. The system records an entry in the Events table indicating the success or failure of the operation.

3.1.18.3. Dependencies

This feature requires the completion of the following before it can begin execution:

- a. System Feature 17, “Detect central computer”
- b. At least one of Features 15, “Accept error records from SecureDRE,” and 16, “Accept error records from CardReader”
- c. At least one of Features 14, “Check voting results for anomalies,” and 21, “Accept recount results”

This feature requires Security Features 6, “Encrypt outbound data,” and 1, “Verify identity of data transmitters.”

3.1.19. System Feature 19: Display precinct election results

3.1.19.1. Purpose of Feature

This feature allows the system to display tallies for candidates for its precinct.

3.1.19.2. Stimulus-Response Sequence

1. The user indicates to the system that he/she wishes to view the tallies for each candidate for the precinct.
2. The system retrieves the entries from the Tallies table of the Database.
3. The system displays the results in a readable format.

3.1.19.3. Dependencies

This feature requires the successful completion of System Feature 14, “Check voting results for anomalies,” before it can begin execution.

This feature requires Security Feature 2, “Encrypt Database tables.” It is restricted by Security Features 3, “Restrict data flow to Database tables,” and 7, “Database login.”

3.1.20. System Feature 20: Detect and log errors

3.1.20.1. Purpose of Feature

This feature allows the system to detect exceptions and errors and store auditable information about them in the Database for later retrieval.

3.1.20.2. Stimulus-Response Sequence

1. While performing an operation, ReliaVote PE encounters an error or exception.
2. ReliaVote PE attempts to write the contents of the system's temporary memory (hereafter the "memory dump") to the hard disk.
3. The system's behavior depends on the type of error that is encountered.
 - a. If it is a non-fatal error, ReliaVote PE records the system error code, identification of the machine where the error occurred, date of the error, and time of the error in the "Events" Database table. ReliaVote PE also records the type of error and an error message, if provided. It then executes Steps 5 – 6.
 - b. If it is a fatal error that requires that ReliaVote PE be restarted, ReliaVote PE attempts to write the error code, date, time, error type, and error message to the hard disk. It then reboots and performs Steps 4 – 6.
4. The software restarts. ReliaVote PE reads the hard disk to determine whether the software experienced a fatal error condition the last time it shut down. Since this was the case, ReliaVote PE reads the memory dump from the hard disk.
5. Using the system state information in the memory dump, ReliaVote PE attempts to continue or restart the operation that was being performed when the error occurred.
6. ReliaVote PE resumes normal operation.

3.1.20.3. Dependencies

This feature requires the completion of no other System Features before it can begin execution. It does require that an error condition occur.

This feature requires Security Features 1, "Verify identity of data transmitters," 2, "Encrypt Database tables," and 6, "Encrypt outbound data."

3.1.21. System Feature 21: Accept and verify recount results

3.1.21.1. Purpose of Feature

This feature allows ReliaVote PE to accept and store the recount results from a CardReader-compatible ballot-scanning machine in the network

3.1.21.2. Stimulus-Response Sequence

1. The system receives a request from a CardReader-compatible ballot-scanning machine to send its recounted vote tallies, updated Ballots table, and “Recount_Votes” Database table.
2. The system sends a response to the machine requesting its data.
3. The system sets itself to be in “Recount Mode.”
4. The system receives the data from the machine.
5. The system checks the Ballots table of its Database to determine if any ballots that it has designated “Archived” have been included in the recount.
Conditional: If the system finds any such ballots, the votes associated with that ballot identification are excluded and the recount tally it received is deducted for each candidate that had been voted for on the archived ballot.
6. The system checks the Ballots table for any non-archived ballots that were not included in the recount (i.e., whose recount flag is not set). Conditional: If the system finds any such ballots, it displays a message to the user to that effect and generates an entry in the Events table but proceeds with the remainder of the steps.
7. The system parses the Recount_Votes table and calculates tallies for each candidate or ballot option.
8. The system compares its tallies to the Recount_Tallies figures. Conditional: If the two figures are different, the system displays a message to the user that the tallies were anomalous and recommends that the user conduct a hand recount. It disallows the addition of the anomalous recount data and exits this operation and generates an error entry in the Events table.
9. The system attempts to add the data to the Database.
10. The system’s operation depends on the result of Step 9.
 - a. If the system successfully added the data to the Database, it transmits a response to the machine that the data were successfully added, records a success entry in the Events table, and executes Step 13.
 - b. If the system failed to add the data to the Database, it transmits a response to the machine that the data were rejected and executes Steps 11 – 13.
11. The system creates an entry in the Events table containing the error code, the machine on which the error occurred, the date and time of the error, and any other error information.
12. The system displays a message to the user that the data were rejected from the Database. This message also contains any error codes and error messages generated by the database management system.
13. The system displays the ReliaVote PE main screen.

3.1.21.3. Dependencies

This feature requires the successful completion of System Feature 11, “End election,” before it can begin execution.

This feature requires Security Features 1, “Verify identity of data transmitters,” 2, “Encrypt Database tables,” 6, “Encrypt outbound data,” and 7, “Database login.” It is restricted by Security Feature 3, “Restrict data flow to Database tables.”

3.1.22. System Feature 22: Display recount results

3.1.22.1. Purpose of Feature

This feature allows the system to display recount tallies for candidates for its precinct.

3.1.22.2. Stimulus-Response Sequence

1. The user indicates to the system that he/she wishes to view the results of a ballot recount.
2. The system queries its Database for the recounted tallies.
3. The system displays the tallies to the user in a readable format.

3.1.22.3. Dependencies

This feature requires the successful completion of System Feature 21, “Accept recount results,” before it can begin execution.

This feature requires Security Features 2, “Encrypt Database tables.” It is restricted by Security Features 3, “Restrict data flow to Database tables,” and 7, “Database login.”

3.1.23. System Feature 23: Clear election results

3.1.23.1. Purpose of Feature

This feature allows the system to remove all vote data and tallies from the Database after an election is over and the data are no longer needed. This operation can be performed *only* after a predetermined period of time after the day set for Election Day. It should be noted here that results cannot be deleted in part; this operation clears the entire Database table. This is an anti-fraud mechanism.

3.1.23.2. Stimulus-Response Sequence

1. The user indicates to the system that he/she wishes to clear the Database of election results.
2. The system checks to ensure that enough time has elapsed and that the operation is allowed. Conditional: If enough time has not elapsed, the system displays a message indicating that the operation cannot be performed and exits this operation.
3. The system attempts to delete all entries from the Votes, Realtime_Votes, Recount_Votes, Tallies, Recount_Tallies, and Ballots tables in the Database.
4. The system records an entry in the Events table indicating the success or failure of the operation.
5. The system displays the ReliaVote PE main screen.

3.1.23.3. Dependencies

This feature requires the successful completion of System Feature 18, “Send results to a central computer,” before it can begin execution.

This feature is restricted by Security Feature 4, “Limit changes to Database on Election Day.” It requires Security Features 1, “Verify identity of data transmitters,” 6, “Encrypt outbound data,” and 7, “Database login.”

3.1.24. System Feature 24: Clear election results from voting devices

3.1.24.1. Purpose of Feature

This feature allows the system to clear the election results of the Database of any voting device on the network. This operation can be performed *only* after a predetermined period of time after the day set for Election Day. It should be noted here that results cannot be deleted in part; this operation clears the entire Database table. This is an anti-fraud mechanism.

3.1.24.2. Stimulus-Response Sequence

1. The user indicates to the system that he/she wishes to clear the election results of one or more SecureDRE-compatible voting machines or CardReader-compatible ballot scanners on the network.
2. The system displays a list of all voting equipment that it has detected.
3. The user selects either a single machine or multiple machines to clear.
4. The system sends the deletion instructions to the selected voting equipment.
5. The system receives a notification from the machine(s) of the machine's success or failure to clear the data.
6. The system's operation depends on the results of Step 6.
 - a. If the notification indicates a success, the system displays a message to the user that the data were successfully deleted from the machine.
 - b. If the notification indicates a failure, the system displays a message to the user that the deletion failed. This message also contains the error code and error message sent by the voting machine.
7. The system records an entry in the Events table detailing the success or failure of the operation.
8. The system displays the ReliaVote PE main screen.

3.1.24.3. Dependencies

This feature requires the successful completion of System Feature 23, "Clear election results," before it can begin execution.

This feature is restricted by Security Feature 4, "Limit changes to Database on Election Day." It requires Security Features 1, "Verify identity of data transmitters," 2, "Encrypt Database tables," 6, "Encrypt outbound data," and 7, "Database login."

3.1.25. System Feature 25: View events

3.1.25.1. Purpose of Feature

This feature allows the user to view the events that have occurred during the course of operation.

3.1.25.2. Stimulus-Response Sequence

1. The user indicates to the system that he or she wishes to view the event log for the software.
2. The software reads the entries in the Events table of the Database and displays this information in read-only format to the user. The software allows the user to dismiss the information.
3. The software processes the user's input from Step 2.
4. The software displays the ReliaVote Precinct Edition main screen.

3.1.25.3. Dependencies

This feature requires the successful completion of System Feature 2, "Login a user," before it can begin execution.

This feature requires Security Feature 7, "Database login."

3.1.26. System Feature 26: Create a new user

3.1.26.1. Purpose of Feature

This feature allows the system to create new usernames with Administrator privileges.

3.1.26.2. Stimulus-Response Sequence

5. The user indicates to the system that he/she wishes to create a new username.
6. The system prompts the user for the username to be created.
7. The user inputs a username to the system.
8. The system determines whether the requested username contains invalid characters. Conditional: If the system finds that the username contains invalid characters, it displays a message to the user and exits this sequence of steps.
9. The system compares the requested username against all existing usernames to determine if it is a duplicate. Conditional: If the system finds that the username already exists, it displays a message to the user and exits this sequence of steps.
10. The system prompts the user for a password for this user.
11. The user inputs a password to the system.
12. The system determines whether the password is sufficiently long. Conditional: If the password is shorter than a predetermined length, the system displays a message to the user and reverts to Step 6.
13. The system assigns the new username Administrator privileges.
14. The system converts the new user's password to a hash value using a hash encryption function.
15. The system stores the username, hashed password, and privilege level in its list of users.
16. The system generates an event in the Events table of the Database.

3.1.26.3. Dependencies

This feature requires the successful completion of System Feature 2, "Login a user," before it can begin execution.

3.1.27. System Feature 27: Change a user's password

3.1.27.1. Purpose of Feature

This feature allows a user who is logged in to change his/her password.

3.1.27.2. Stimulus-Response Sequence

1. The user indicates to the system that he/she wishes to change his/her password.
2. The system prompts the user for a new password.
3. The user inputs a password to the system.
4. The system determines whether the password is sufficiently long.
Conditional: If the password is shorter than a predetermined length, the system displays a message to the user and reverts to Step 2.
5. The system prompts the user to re-enter the password to confirm it.
6. The user inputs the password to the system.
7. The system determines whether the password is the same as the first password that the user input. Conditional: If the passwords are different, then the system displays a message to the user and exits this sequence of steps.
8. The system converts the new password to a hash value using a hash encryption function.
9. The system replaces the old hashed password with the new one in the list of users.
10. The system generates an event in the Events table of the Database.

3.1.27.3. Dependencies

This feature requires the successful completion of System Feature 2, "Login a user," before it can begin execution.

3.1.28. System Feature 28: Delete a user

3.1.28.1. Purpose of Feature

This feature allows a user to delete another username from the list of users. The system does not allow the user to delete the username that is currently logged in; this is to ensure that there is always at least one username that can login to the system.

3.1.28.2. Stimulus-Response Sequence

1. The user indicates to the system that he/she wishes to delete a username.
2. The system displays the list of all usernames to the user. The system also provides the user with the opportunity to cancel the operation.
3. The user makes a single selection on the list.
4. The system prompts the user to confirm the deletion of the selected username. The system also provides the user with the opportunity to cancel the operation.
5. The user indicates to the system that he/she wishes for the username to be deleted.
6. The system determines if the username to be deleted is currently logged in.
Conditional: If the username is currently logged in, the system does not allow the deletion. It displays a message to the user and exit this sequence of steps.
7. The system removes the username, password, and privilege level from the list of users.
8. The system generates an event in the Events table of the Database.

3.1.28.3. Dependencies

This feature requires the successful completion of System Feature 2, “Login a user,” before it can begin execution.

3.1.29. System Feature 29: Manually logout a user

3.1.29.1. Purpose of Feature

This feature allows the system to logout a user. ReliaVote Precinct Edition allows only one user at a time to be logged in; if a user wishes to use the software when another one is logged on, the current one must logout first.

3.1.29.2. Stimulus-Response Sequence

1. The user indicates to the system that he/she wishes to logout.
2. The system allows any currently executing functions to finish and terminates any that are not responding.
3. The system terminates the user's session.
4. The system creates an entry in its Events table that the username has logged out. This entry also contains the date and time of the logout.

3.1.29.3. Dependencies

This feature requires the successful completion of System Feature 2, "Login a user," before it can begin execution.

3.1.30. System Feature 30: Automatically logout a user

3.1.30.1. Purpose of Feature

This feature allows the system to automatically terminate a user session when the system has been idle for a certain period of time. This allows for security in case the computer is left unattended for extended periods of time.

3.1.30.2. Stimulus-Response Sequence

1. The system begins a timer after a given period in which none of the system events detailed in this document have executed.
2. If a system event executes, the system stops the timer and exits this sequence of steps.
3. If the timer reaches a predetermined number, the system automatically logs out the user that is logged in.
4. The system allows any currently executing functions to finish and terminates any that are not responding.
5. The system terminates the user's session.
6. The system creates an entry in its Events table that the username has logged out. This entry also contains the date and time of the logout.

3.1.30.3. Dependencies

This feature requires the successful completion of System Feature 2, "Login a user," before it can begin execution.

3.2. Performance Requirements.

The features described in this section are requirements that are necessary for ReliaVote Precinct Edition to perform in a reasonable amount of time.

3.2.1. Performance Requirement 1: Modify Database quickly

Numerous features of ReliaVote Precinct Edition require changes to be made to the Database. Any operations involving the Database must take place in an amount of time that would be unnoticeable to a typical user of the software.

As is described in §3.3, subsections, numerous operations require that parts of the Database employ cryptography for data protection and machine identity verification. The cryptographic algorithms used must be executed in a reasonable amount of time and be unnoticeable to a typical user.

3.2.2. Performance Requirement 2: Transmit and receive data quickly

ReliaVote Precinct Edition has to receive, transmit, and process large amounts of data. This requires that the computer have access to a broadband Internet connection and a fast link between it and all machines with which it will exchange data. ReliaVote Precinct Edition itself must be able to accept the large amounts of data without slowing its processing excessively or losing any of the data.

3.3. Security Requirements.

The features described in this section are requirements that are necessary to ensure the integrity of election data generated and stored by the ReliaVote Precinct Edition software product.

3.3.1. Security Feature 1: Verify identity of data transmitters

3.3.1.1. Purpose of Feature

This feature restricts the sources of data that will be allowed to perform privileged operations on ReliaVote PE. The precinct computer (see §3.3.5) limits access to the private network, but in the event that it should fail, this security feature protects the Database from malicious operations. It requires that any data transfers processed by ReliaVote PE must have originated at the central computer or a voting device located on the precinct's network.

3.3.1.2. Characteristics of Feature

When any data transfers are received, the system will check to ensure that they have been encrypted. The details of this system are given in reference [5], *Network Detailed Design*.

The keys will be managed by a Kerberos-compatible key management system. Systems whose keys the ReliaVote PE system will need are the county's central computer, all voting devices on the private network, and the system itself.

If ReliaVote PE determines that a packet was sent by the machine it appears to be from and intended for the machine that received it, then the packet will be processed. Otherwise, the packet is discarded.

3.3.2. Security Feature 2: Encrypt Database tables

3.3.2.1. Purpose of Feature

This feature provides for encryption of sensitive Database tables in the ReliaVote PE internal Database.

3.3.2.2. Characteristics of Feature

The Votes, Realtime_Votes, and Recount_Votes tables in the Database are highly sensitive and must be protected with encryption of at least 128-bit strength when not being modified. This encryption scheme can be symmetric or asymmetric; the two options are detailed in reference [3]. The keys to this encryption system must not be known or recoverable by human users.

The entire table is encrypted rather than individual entries. This means that it is not possible to add, modify, or delete entries while the table is encrypted.

When the System initiates an operation that involves one of these tables, it decrypts the affected table, performs the operation, generates a new key, and re-encrypts the table with the new key. This means that the key is changed every time an operation is performed on one of the tables. The software generates different keys for each table.

3.3.3. Security Feature 3: Restrict data flow to Database tables

3.3.3.1. Purpose of Feature

This feature restricts traffic to sensitive tables in the Database.

3.3.3.2. Characteristics of Feature

The Votes, Realtime_Votes, and Recount_Votes tables in the Database are highly sensitive. In addition to being protected by strong encryption and secret keys, they are protected from access by operations that did not originate on the local computer. ReliaVote PE analyzes all incoming data packets to determine if they contain instructions to modify or view either of these tables. If the packets contain modification instructions, then the instructions contained therein are processed only if they originated on a voting machine in the precinct's network. Otherwise, the packets are discarded. ReliaVote CS should not be generating such packets (ref. [6]), and their presence could indicate that the system has been compromised. Likewise, the only system that needs to receive copies of precinct-level vote tallies is the central server, and packets containing such requests are processed only if they originated on that computer. All packets that involve Database operations are "repackaged" by the ReliaVote PE software as a ReliaVote PE operation, so that the Database will recognize and execute them.

3.3.4. Security Feature 4: Limit changes to Database on Election Day

3.3.4.1. Purpose of Feature

This feature restricts user access to particular tables in the Database for a time period on and immediately after Election Day.

3.3.4.2. Characteristics of Feature

The Database contains numerous tables containing information about candidates, contests, and political parties. These tables can be modified by Administrators until 12:00 A.M. on Election Day. At this time all of the Database will be locked from modification (except for the Ballots, Votes, Realtime_Votes, Tallies, and Events tables) for a given period of time after Election Day ends. Only the System user can modify these tables during this lockdown.

3.3.5. Security Feature 5: Virtual private network

3.3.5.1. Purpose of Feature

This feature requires that the precinct computer running ReliaVote PE must manage a virtual private network (VPN) between the precinct's private network and the public Internet. The precinct computer will be the communication point between the public Internet and the private network.

3.3.5.2. Characteristics of Feature

In a precinct, all MyVotronics and any other election equipment (hereafter "nodes") will be connected to the Internet via a private network. The only node with direct access to public IP addresses will be the precinct computer. The precinct computer will filter traffic that is destined for private nodes. If a data transmission from the county's computer requests that the precinct computer initiate an operation on a private node, then the precinct computer will generate a new data transmission for the intended node, with its own IP address as the source rather than the central computer's. (It should be noted that the destination node will still discard the data packet if it contains instructions to modify a sensitive Database table.) Traffic destined for a private node originating from any other IP address is dropped.

Appendix A provides a graphical depiction of the proposed network design. Reference [5], *InnoVote Network Detailed Design*, contains detailed network prototypes and suggested network rules.

3.3.6. Security Feature 6: Encrypt outbound data

3.3.6.1. Purpose of Feature

This feature requires that all data transfers destined for a machine external to the precinct computer must be encrypted.

3.3.6.2. Characteristics of Feature

All outbound data transmissions from ReliaVote PE will be protected with encryption of at least 192-bit strength.

The feature utilizes the same cryptosystem described in Security Feature 1.

3.3.7. Security Feature 7: Database login

3.3.7.1. Purpose of Feature

This feature requires that all accesses of the Database be made by a verified “user” that the database management system recognizes. This is to prevent unauthorized SQL querying.

3.3.7.2. Characteristics of Feature

The database management system will recognize the ReliaVote PE software as a “user.” The software must authenticate itself when it makes any modification to the Database. The database management system will not permit anonymous SQL querying.

3.3.8. Security Feature 8: Block all ports except three

3.3.8.1. Purpose of Feature

This feature requires all data ports on the precinct computer will be blocked from sending and receiving data transmissions except for one over which the System will exchange data with the county computer, one for communication with the county Kerberos server, and one for the precinct Kerberos server.

3.3.8.2. Characteristics of Feature

ReliaVote PE will initiate connections on one data port, and this port will be used only by InnoVote software. Additionally, the client installation of Kerberos software will use data ports to communicate with the key servers for the precinct and county networks. A hardware firewall will be configured to disallow traffic originating from or destined for any port other than the chosen ones. The firewall must not permit any configurations that would permit incoming or outgoing traffic from ports other than these on the computer running ReliaVote PE. More information about this is present in *Network Detailed Design* [4].

3.4. System Attributes

The attributes described in this section are, unless otherwise stated, general to the ReliaVote PE software product rather than specific to a particular system feature.

3.4.1. Reliability

The ReliaVote PE software must experience normal exception-free behavior at least 99.999 percent of the time. This would correspond to no more than one exception within a 24-hour period.

3.4.2. Availability

The ReliaVote PE software will execute on a computer, and all users must be physically present to use it. Remote logins are not permitted. Availability is not an issue with this software product.

3.4.3. Security

The security requirements of ReliaVote Precinct Edition are detailed in §3.3, “Security Features.”

3.4.4. Maintainability

The system must be upgradable if necessary. Any upgrades must require no changes to the existing relational schema for the Database. They must not compromise any Security Features of the software.

3.4.5. Portability

The software must execute on any Intel- or Macintosh-compatible uniprocessor computer system.

4. Appendices

Appendix A: Precinct-Level Network Diagram for InnoVote Products

