InnoVote Election Products

Systems Overview

By
Erin Thead
Software Engineer
erin@erinthead.com

Table of Contents – InnoVote Systems Overview

1. Introduction

1.1. Purpose

The purpose of this document is to detail an overview of the hardware and software components of the InnoVote™ election system product line. The document provides a brief description of the general purpose of each product and how it fits with the other InnoVote products.

The document also contains an overview of data-storage and networking specification documents. The InnoVote products depend heavily on data storage and network communication, and their requirements are tailored for specific configurations.

1.2. References.

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

1.3. Definitions, Acronyms, and Abbreviations

- CardReader Hardware: The ballot-scanning equipment on which CardReader Software will execute. A hardware schema is provided in Part 1.
- CardReader: The software that controls the InnoVote CardReader hardware, whose attributes are defined in Part 5. ("CardReader" always refers to the software; when the hardware is intended, the term "CardReader hardware" is used.) "CardReader-compatible" refers to a software product that can perform the same functions as InnoVote CardReader.
- County computer: The computer in a County central election office that is running central tabulation software, in this document assumed to be ReliaVote CS.
- County: Refers to either a county or parish in a state.
- Cryptosystem: A protocol or implementation that uses secrets such as passwords or keys to authenticate individuals and/or provide confidentiality to data.

- Database management system: The software that is used to establish, configure, and maintain a database.
- DBMS: Database management system.
- Database: Refers to any relational database stored on an InnoVote product. All InnoVote products' databases use the same relational schema, which is defined in Part 3, so "Database" can refer to any database used by an InnoVote software product.
- DRE: Direct Recording Electronic voting machine.
- Error: A condition in which the system either experiences an exception or in which an attempt to violate a security rule occurs.
- Exception: An error in which the system fails to function as expected.
- InnoVote: Working name of the product line.
- IP: Internet Protocol, the standard protocol used in the Internet. IP version 6 is the preferred version for InnoVote products.
- Kerberos: An authentication protocol that validates the identity of both a sender and a receiver of data. This protocol allows for fully encrypted network transmissions. Part 4 gives a detailed description of the InnoVote implementation of this protocol.
- Machine: Used by itself with no other context (e.g., "voting machine"), this term refers to any computer or voting device.
- MyVotronic OS: The operating system for the MyVotronic machine.
- MyVotronic: The DRE machine on which SecureDRE will operate, for which a brief hardware requirement specification can be found in Part 2. "MyVotronic-compatible" refers to a hardware product that can perform the same functions as the MyVotronic DRE machine.
- Packet: The basic unit of data transmitted over a network. A packet's size depends on various characteristics of the network, as well as the amount of data being sent.
- Precinct computer: The computer in a Precinct that is running ReliaVote PE.
- Precinct server: Synonymous with "precinct computer."
- Precinct: Refers to the physical site at which people cast ballots on Election Day, whether *called* a "precinct" by local government or not.
- Public key cryptosystem: A system of cryptography in which each user (person, computer, network node) has a private encryption key that only it can use, plus a public encryption key that others can obtain and use to ensure that only the user with the matching private key can decrypt the sensitive data.
- RAM: Random Access Memory, the memory of a computer that requires electrical power to retain data. Synonymous with "temporary memory."
- ReliaVote CS: ReliaVote Central Server, the software operating on a central computer in each county, whose attributes are defined in Part 6. "ReliaVote CS-compatible" refers to a software product that can perform the same functions as the ReliaVote Central Server software.
- ReliaVote PE: ReliaVote Precinct Edition, the software operating on a computer in each precinct, whose attributes are defined in Part 7. "ReliaVote PE-compatible" refers to a software product that can perform the same functions as the ReliaVote Precinct Edition software.

- SecureDRE: The election software that executes on the InnoVote MyVotronic hardware. Its attributes are defined in Part 8. "SecureDRE-compatible" refers to a software product that can perform the same functions as the SecureDRE software.
- Software Gateway: A term to indicate that a particular software component does not make direct connections to any network and the only means to access it remotely is through another software product. This term is used only in Part 3, the *Database Detailed Design*, and it is used to describe the configuration of an InnoVote Database stored on any InnoVote election product. These Databases do not connect to the network and do not accept remote connections; the only "gateway" to access them remotely is through an InnoVote software product.
- Software: When capitalized, refers to the specific software product being described in a Functional Design document.
- SQL: Structured Query Language, the language that a relational database recognizes and which is used to perform operations on a relational database.
- System: When capitalized, synonymous with "Software."
- TCP/IP: Transmission Control Protocol/Internet Protocol, the protocols used for most data transfers on the Internet at the transport and network layers.
- VPN: Virtual Private Network, a networking configuration in which computers located on public networks obtain a secure communication channel between each other.

1.4. Overview.

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

Section 2: Contains a listing and brief overview of the basic purpose of each InnoVote product.

Section 3: Contains an overview of the network and database compatibility capabilities of the products.

Section 4: Contains a brief description of the rest of the documentation for the InnoVote products.

2. Overview of InnoVote Election Products

2.1. InnoVote CardReader Hardware.

The InnoVote CardReader is a scanning machine that reads paper ballots and transmits them via a Universal Serial Bus (USB) or other connection to a computer for storage and further transmission. In case of connection errors between the scanner and the computer, the CardReader ballot scanner contains its own microprocessor and memory. It is capable of storing failed USB transmissions in a queue until it detects a connection to a computer running the CardReader software product.

The computer system that controls the CardReader scanner is a kiosk-type system with no keyboard or mouse and no software applications other than system processes and the CardReader Software. In addition to its single USB connection with the scanner, it contains an Ethernet adapter, over which it exchanges data with the precinct's central computer and the cryptographic key server for the precinct. Except for error detection and logging, all operations on CardReader are initiated either by an authenticated data transmission from the precinct computer or by data input from the CardReader scanner.

Throughout these documents, the term "CardReader hardware" is used to refer either to the scanner by itself or to the scanner-computer combination. The context should make clear which is intended.

2.2. InnoVote CardReader Software.

InnoVote CardReader Software is a software product that executes on a computer that is connected via USB to a CardReader ballot scanner. The software controls and processes scanner input/output, storing vote data in a database on the hard disk of the computer. It also controls and filters data exchange with a central computer in the voting site where the scanner is located. As is indicated in the Functional Design document for CardReader, software operations can be initiated only by input from the ballot scanner or from this precinct central computer; CardReader does not process input from any other hardware devices.

2.3. InnoVote MyVotronic Direct Recording Electronic Voting Machine.

The MyVotronic Direct Recording Electronic (DRE) voting machine is a secure, accountable electronic voting machine. It contains a printer to produce a paper ballot for equal protection under the law. It also contains components to accept input from voters via a touchscreen, a simplified keyboard (for write-in candidates), and a bar code scanner that permits changes to votes after a ballot has been printed. MyVotronic is a self-contained system that can store data indefinitely; however, for full correct operation of the hardware (and for correct conduct of an actual election), it contains an Ethernet adapter that connects it with a central computer in its precinct. The machine exchanges data with this precinct computer and with the cryptographic key server for its precinct.

MyVotronic's operating system is called MyVotronic OS. It controls MyVotronic hardware input/output and manages access controls to data. The documentation for all InnoVote Products assumes that MyVotronic OS will be the actual operating system that is deployed on the MyVotronic. If, in deployment, the hardware components for MyVotronic are chosen and configured in such a way as to allow an existing third-party operating system to be usable, then certain details of the documents that relate to MyVotronic OS compatibility issues will not be applicable.

2.4. InnoVote ReliaVote Central Server Software.

ReliaVote Central Server is a vote tabulation software product that executes on a computer in a central location in the county or parish. It accepts and processes authenticated data transmissions from ReliaVote Precinct Edition software, the general-purpose election software that executes on computers in each voting site or "precinct." ReliaVote Central Server requires a database and database management system.

2.5. InnoVote ReliaVote Precinct Edition Software.

ReliaVote Precinct Edition is a complex election-management software product that executes on a computer in a voting site or "precinct." It initiates many operations of the CardReader and SecureDRE/MyVotronic products, including "programming" the election databases on every voting device in its precinct-level network. It accepts and validates election data from its precinct and transmits validated data to the next level, i.e., the ReliaVote Central Server computer for the county or parish. ReliaVote is able to filter data from external sources and blocks certain operations from being performed on its own database. As with ReliaVote Central Server, ReliaVote Precinct Edition requires a database and database management system.

2.6. InnoVote SecureDRE Software.

SecureDRE is the voting software that executes on the MyVotronic hardware. SecureDRE displays ballots in electronic form and reads input from voters, storing it in the database on the voting machine before transmitting a copy to the precinct computer. It can also receive data from the precinct computer. SecureDRE sends output to the MyVotronic printer and accepts input from the bar code scanner.

2.7. InnoVote Databases.

All InnoVote software products will use a database to store election data and error reports. Each physical machine—either a computer or a MyVotronic voting machine—will have its own local database. Some systems will transmit parts of their databases to other InnoVote systems over a secure network connection, and this necessitates that the database design be the same for every deployment.

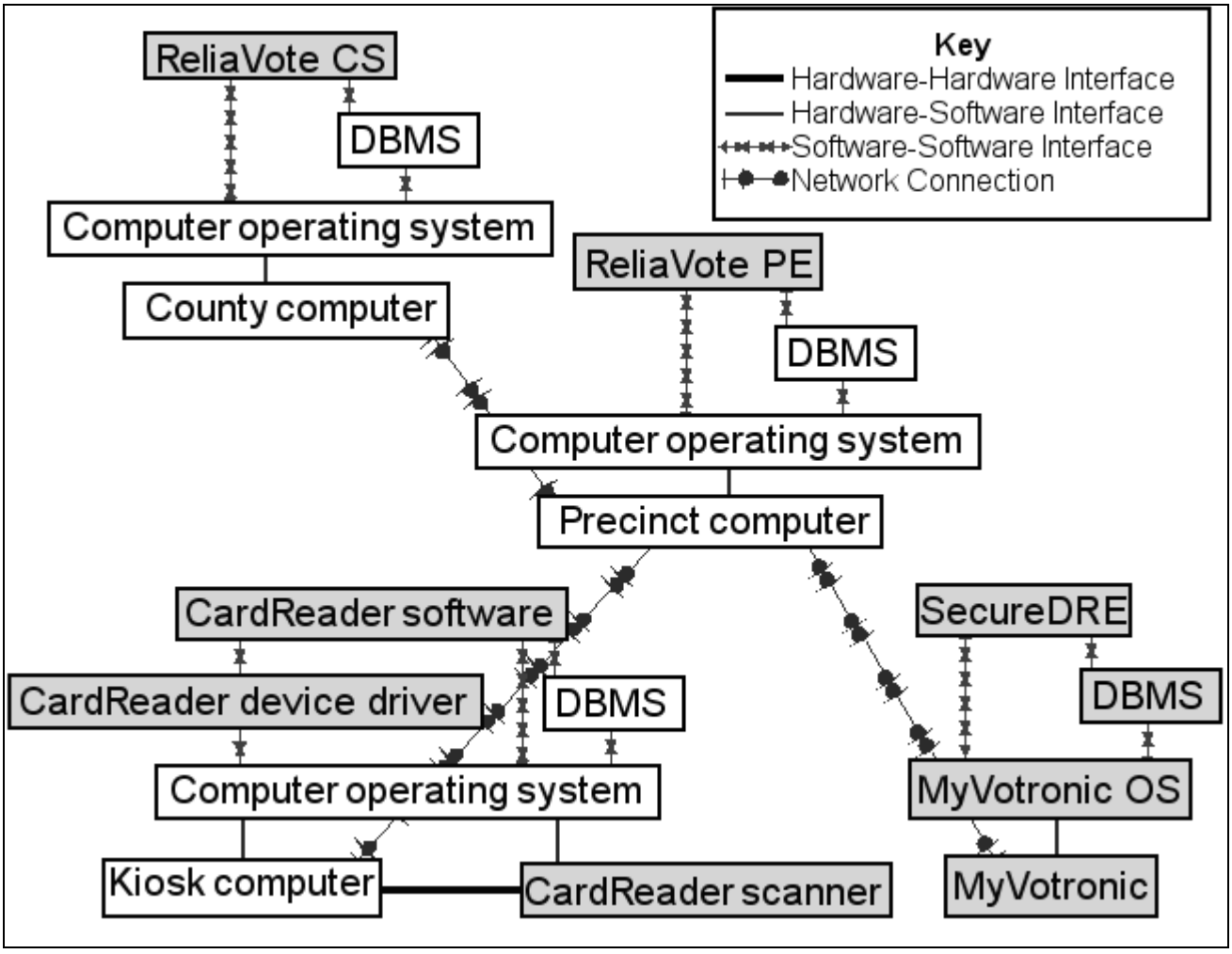
In most cases, the database management system software will be installed on a PC or Macintosh® computer and can therefore be any secure commercial database product that meets the requirements of the *Database Detailed Design* document. However, these documents assume that the MyVotronic voting machine has a custom operating system called MyVotronic OS. This design requires that the database software used on MyVotronic be customized to be compatible both with MyVotronic OS and with the third-party database software used by the other systems. It may be possible to build the MyVotronic machine in such a way that some existing third-party operating system will meet the requirements of the *MyVotronic Hardware and Operating System Overview* document and the custom operating system will not have to be built. If this is the case, then the database software can be the same as that deployed on the other products. However, the developer does not make such an assumption in these documents.

2.8. Deployment of InnoVote Products.

Figure 1 shows a suggested deployment configuration for InnoVote products. Light gray boxes represent InnoVote products; white boxes are non-InnoVote systems that InnoVote products will use. Any designation of "Computer operating system" refers to a commercial or open-source operating system (such as Microsoft® Windows®, Apple® OS X®, or Linux®) that can be installed on a commercially available computer.

The term "interface" refers to a means by which one component can exchange information with another. Despite the appearance of the diagram, the network connections are between network adapters installed on hardware devices, not software components.

Figure 1: InnoVote Products Deployment Diagram



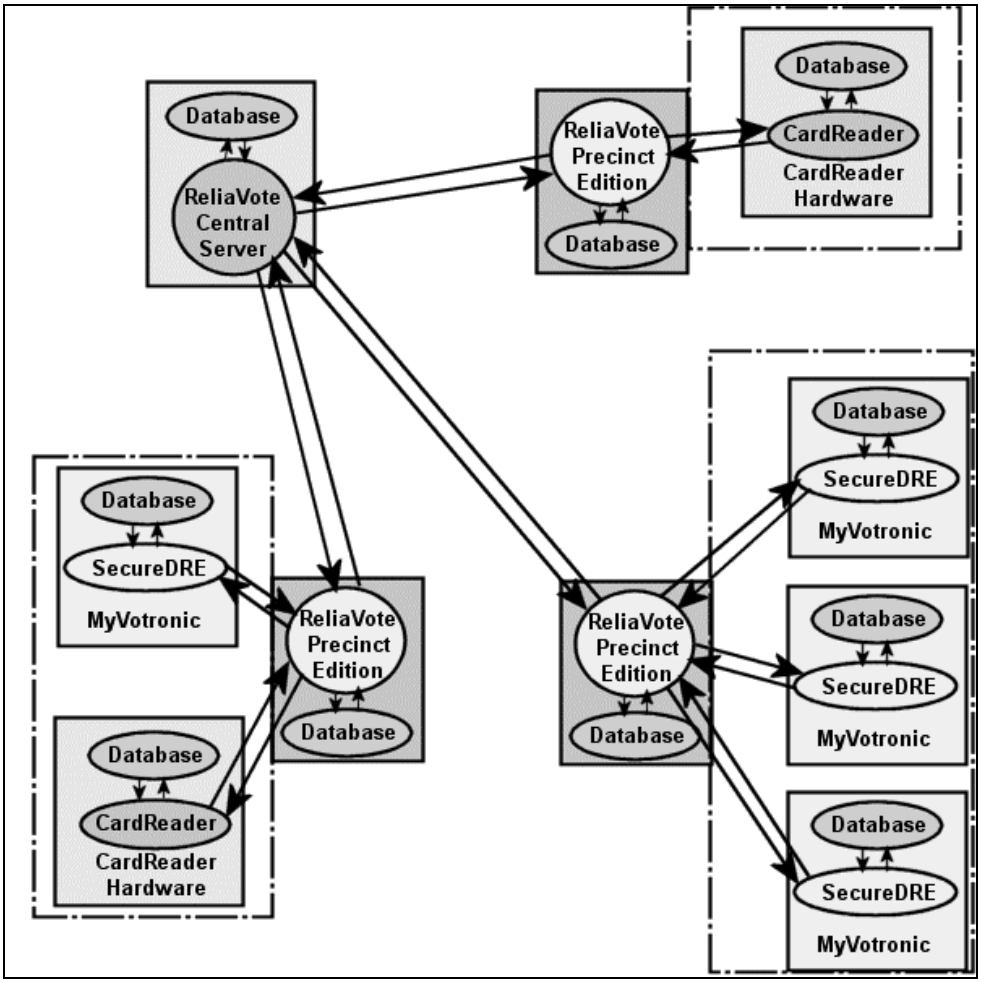
3. Cross-compatibility of InnoVote Election Products

3.1. County-level Networking.

Every InnoVote product is designed to be networked with other InnoVote (or compatible) products. CardReader and MyVotronic/SecureDRE systems are designed to exchange data with ReliaVote Precinct Edition software at the precinct or voting-site level. ReliaVote exchanges data both at the precinct level and the county level, with the ReliaVote Central Server software. ReliaVote Central Server exchanges data only with ReliaVote Precinct Edition.

Figure 1 shows a simple county-wide network of InnoVote products. In the diagram, arrows on solid connecting lines indicate the direction of permitted data transfers between components. Solid rectangles represent hardware devices, ovals represent software components, and dashed lines represent private precinct-level networks.

Figure 2: InnoVote Products Network Overview



3.2. Database Compatibility.

As is shown in Part 3 of the documentation, “Database Detailed Design,” InnoVote products use the same relational schema for their database, so all databases stored on InnoVote products are compatible with each other and can exchange table entries.

Under correct operation, the county’s central computer has a database that contains entries of all ballot options for every precinct in the county, so it can accept valid input from any precinct computer in its county.

Also under correct operation, all databases on voting equipment located in the same precinct contain the same entries in all database tables except those tables that store data for ballots, votes, tallies, and system errors.

The schema of the database is designed such that unusual input (e.g., votes for candidate/contest combinations—other than write-ins—that do not appear on the ballot) is disallowed and an error is generated and entered in the error table.

4. Overview of the Documents

4.1. Part 1: CardReader Hardware Requirements Overview

The CardReader Hardware Requirements Overview contains a description of the basic hardware operations that CardReader machines must perform. It also contains a brief description of the high-level hardware components needed to perform these operations and a design diagram of the hardware structure. The document provides requirements for a device driver for the CardReader optical scanner, which will be necessary for correct interfacing with the computer connected to the scanner and thus correct operation of the CardReader software.

4.2. Part 2: MyVotronic Hardware and Operating System Overview

The MyVotronic Hardware and Operating System Overview contains a description of the basic hardware operations that MyVotronic machines must perform. It also contains an overview of the high-level hardware components needed to perform these operations and a design diagram of the hardware structure. This document is both a hardware design document and an operating system requirements specification for the low-level hardware control operations of the "MyVotronic OS" operating system.

4.3. Part 3: Database Detailed Design

The Database Detailed Design contains a detailed design for the databases that the software products will use. The document provides a description of the databases' structure, rules, data protection, and user authentication mechanisms.

4.4. Part 4: Network Detailed Design

The Network Detailed Design contains a suggested design for the various communication networks that the election products will use to communicate with remote machines. The document provides a description of the network architectures, data flow restrictions, and cryptographic systems of the networks.

4.5. Part 5: CardReader Functional Design

The CardReader Functional Design (FD) provides a detailed description of the functional, performance, and security requirements for the CardReader ballot-scanning and ballot-tabulation software.

4.6. Part 6: ReliaVote Central Server Functional Design

The ReliaVote Central Server FD provides a detailed description of the functional, performance, and security requirements of the ReliaVote Central Server (CS) election software.

4.7. Part 7: ReliaVote Precinct Edition Functional Design

The ReliaVote Precinct Edition FD provides a detailed description of the functional, performance, and security requirements of the ReliaVote Precinct Edition (PE) election software.

4.8. Part 8: SecureDRE Functional Design

The SecureDRE FD provides a detailed description of the functional, performance, and security requirements of the SecureDRE software as it relates to interaction with a voter or with ReliaVote Precinct Edition.

4.9. Part 9: Database Access Matrix

The Database Access Matrix provides a table of the operations that every functional requirement of the four InnoVote software products (CardReader Software, ReliaVote CS, ReliaVote PE, and SecureDRE) will be allowed to perform on each table of an InnoVote database located on the same system as the software. This access matrix relates to security design of InnoVote products.

4.10. Part 10: Security Analysis of InnoVote Products

The Security Analysis provides an explanation of security risks to an electronic election, software and hardware designs of InnoVote products that limit or eliminate these risks, and vulnerable points in the proposed election system.