InnoVote MyVotronic

Hardware and Operating System Overview

By
Erin Thead
Software Engineer
erin@erinthead.com

Table of Contents – MyVotronic Hardware and Operating System Overview

1. Introduction

1.1. Purpose.

The purpose of this document is to communicate an overview of the hardware requirements for the InnoVote MyVotronic direct recording electronic (DRE) voting machine. The document provides a description of required hardware components and basic hardware operations that the components must be able to perform.

In addition to an overview of the hardware design, this document also provides basic requirements for low-level operating system functions. The parts of this document that address software control of hardware components are applicable to low-level design of the operating system, "MyVotronic OS."

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

1.2. Scope.

InnoVote MyVotronic is one component of an interoperable line of products. It is a direct recording electronic voting machine that contains the required hardware features for certain election accountability features of SecureDRE [ref. 6] to operate.

The MyVotronic is similar in most respects to existing voting machines; however, as described in section §2.4, it contains features that do not exist on all (for some features, *any*) currently manufactured products.

The proposed design does not require the development of new technologies. It uses existing hardware components and technologies. For this reason, this document does not provide detailed electrical schematics for the hardware, but rather, an overview of the basic hardware operations that MyVotronic must perform to be fully compatible with SecureDRE and equivalent software and thus provide the full accountability and security that is warranted.

MyVotronic OS is the proposed operating system for the MyVotronic hardware. This document assumes that MyVotronic OS is the operating system actually deployed on the MyVotronic.

1.3. Definitions, Acronyms, and Abbreviations.

- ASCII: American Standard Code for Information Interchange, a single-byte character encoding system used widely in computers.
- 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.
- Database: Refers to any relational database stored on an InnoVote product. All InnoVote products' databases use the same relational schema, so "Database" can refer to any database used by an InnoVote software product.
- Database management system: The software that is used to establish, configure, and maintain a database.
- DRE: Direct Recording Electronic voting machine.
- 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.
- MyVotronic: The DRE machine on which SecureDRE will operate. "MyVotronic-compatible" refers to a hardware product that can perform the same functions as the MyVotronic DRE machine.
- MyVotronic OS: The operating system for the MyVotronic 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: Refers to the physical site at which people cast ballots on Election Day, whether *called* a "precinct" by local government or not.
- RAM: Random Access Memory, the memory of a computer that requires electrical power to retain data. Synonymous in this document with "temporary memory."
- ReliaVote CS: ReliaVote Central Server, the software operating on a central computer in each county, whose attributes are defined in reference [4]. "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 reference [5]. "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 high-level attributes are defined in reference [6]. "SecureDRE-compatible" refers to a software product that can perform the same functions as the SecureDRE software.
- TCP/IP: Transmission Control Protocol/Internet Protocol, the protocols used for most data transfers on the Internet at the transport and network layers.

1.4. References.

[1] Thead, E. *InnoVote Database Access Matrix*, 2005.
[2] Thead, E. *InnoVote Database Detailed Design*, 2005.
[3] Thead, E. *InnoVote Network Detailed Design*, 2005.
[4] Thead, E. *InnoVote ReliaVote Central Server Functional Design*, 2005.
[5] Thead, E. *InnoVote ReliaVote Precinct Edition Functional Design*, 2005.
[6] Thead, E. *InnoVote SecureDRE Functional Design*, 2005.
[7] Thead, E. *Security Analysis of InnoVote Products*, 2005.

1.5. Overview.

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

Section 2: Contains a brief overview of operations that the hardware will need to perform and a high-level description of necessary hardware components.

Section 3: Contains a detailed description of hardware operations, including the hardware components that will be involved in each operation.

2. Overall Description

2.1. Hardware Functions.

The MyVotronic direct recording electronic voting machine must be able to perform the following hardware operations:

1. Power on
2. Charge a replaceable battery
3. Perform standard mathematical and string operations on data
4. Write data to temporary memory
5. Read data from temporary memory
6. Accept input from a touchscreen device
7. Accept input from a modified keyboard
8. Accept input from a network adapter
9. Send output to a network adapter
10. Accept input from an optical scanner
11. Store data on a magnetic disk
12. Retrieve data from a magnetic disk
13. Delete data from a magnetic disk
14. Physically erase data from a magnetic disk
15. Send output to a screen
16. Send output to a printer
17. Regulate the temperature of the system
18. Maintain record of the condition of the battery
19. Display the condition of the battery
20. Perform emergency backups
21. Maintain an internal clock
22. Power off

2.2. Hardware Components.

The MyVotronic direct recording electronic voting machine will require at least the following hardware components:

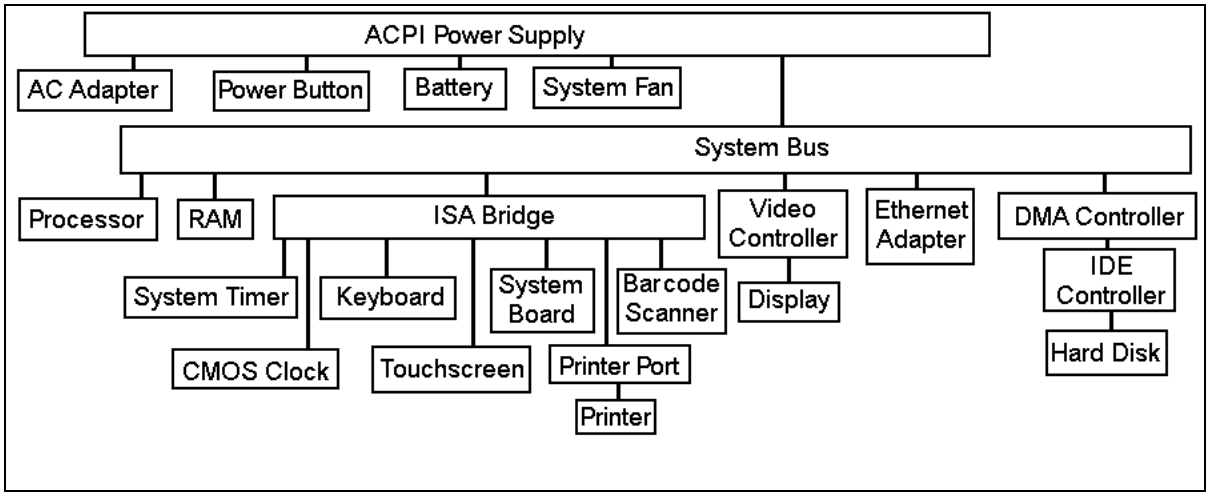
- Advanced Configuration and Power Interface (ACPI)-compliant power supply
- AC adapter
- Lithium ion battery
- Power on/off button
- Cooling fan
- Thermal sensor
- System bus

- Microprocessor
- Random-access memory (RAM)
- Direct Memory Acecss (DMA) module and controller
- Integrated device electronics (IDE) controller
- Hard disk
- System board
- System (CMOS) clock
- System timer
- CMOS battery
- Modified keyboard
- Display adapter (or Video adapter)
- Display screen
- Touchscreen
- Printer port and printer
- Bar code scanner

2.3. Component Diagram for MyVotronic.

Figure 1 shows a diagram of the components that MyVotronic requires. Boxes represent hardware components. Connecting lines represent bidirectional data flow between one component and another, or, in the case of the ACPI Power Supply and the hardware devices to which it is directly connected, the connecting lines represent the flow of electrical current from the power supply to another device.

Figure 1: Component Diagram.



2.4. Differences Between MyVotronic and Existing Voting Machines.

The MyVotronic hardware design is similar to existing voting machines, with three notable exceptions:

- Modified keyboard: The MyVotronic hardware contains a special keyboard to allow write-in candidates to be entered electronically and printed on the ballot/receipt. This keyboard contains the letters of the English alphabet, the space bar, the hyphen, the period, the comma, and the apostrophe. The keyboard will not contain any other keys. Because of the absence of a Shift or Caps Lock key, the names of write-in candidates will be input in capital letters.
- Printer: Some voting machines *do* contain printing devices that print a receipt or "paper trail." The MyVotronic hardware also contains one of these. The printer is internal to the voting machine but easily serviceable for paper replacements. It can be a thermal printer similar to that on a fax machine, or an ink-based printer. If it is uses ink, the printer must be designed so that ink cartridges can be easily serviced.
- Bar code scanner: For accountability purposes, the SecureDRE voting software stores a record of individually cast votes rather than just accumulated tallies. For equal protection as required by United States law, ballots cast on an electronic voting machine must be modifiable until the voter is satisfied with his/her choices. The SecureDRE software provides for modification of votes even after the MyVotronic printer has printed a receipt; this feature is performed easily enough because every ballot is uniquely identifiable by the machine by means of a bar code. The MyVotronic contains a bar code scanner that reads a ballot bar code and converts it to a digital/binary format for processing.

2.5. User Classes.

MyVotronic OS will have a relatively simplistic user privilege model. Most of the security measures to protect the election data from tampering are implemented in the SecureDRE software and the database management system for the MyVotronic's database. However, the operating system does need to distinguish between classes of "users."

2.5.1. Operating System

MyVotronic OS itself is a user class. As with any operating system, it must be able to perform any operation on any hardware component. It must be able to grant and revoke user privileges for other user classes. The Operating System will handle hardware resource requests from other users and allocate or deallocate as its programming dictates.

2.5.2. General User

MyVotronic OS does not provide for user logins; however, any instance of a software product (including SecureDRE) executing on a MyVotronic machine is granted General User privileges by the Operating System.

A General User cannot seize any hardware resource currently being utilized by another General User. If a General User needs to use a hardware resource, it must make a request to the Operating System, which then may grant or deny the request.

2.5.3. "Dirty" Data

Any data received from a network adapter are marked by the Operating System as "dirty." This designation applies to encrypted and nonencrypted data. The Operating System will not allow dirty data to be executed as instructions.

If the dirty data arrive when the Operating System is not processing any General User's request for the network adapter, the Operating System assumes that the packets are untrustworthy and discards them. This is a valid assumption if SecureDRE is installed on the system; if SecureDRE is executing, then it has been granted General User privileges and will have requested the network adapter almost immediately. (As shown in [6], its first operation upon loading is to identify itself on the network, an operation that requires the network adapter.) After SecureDRE has loaded, it is the only user with a legitimate need for external data.

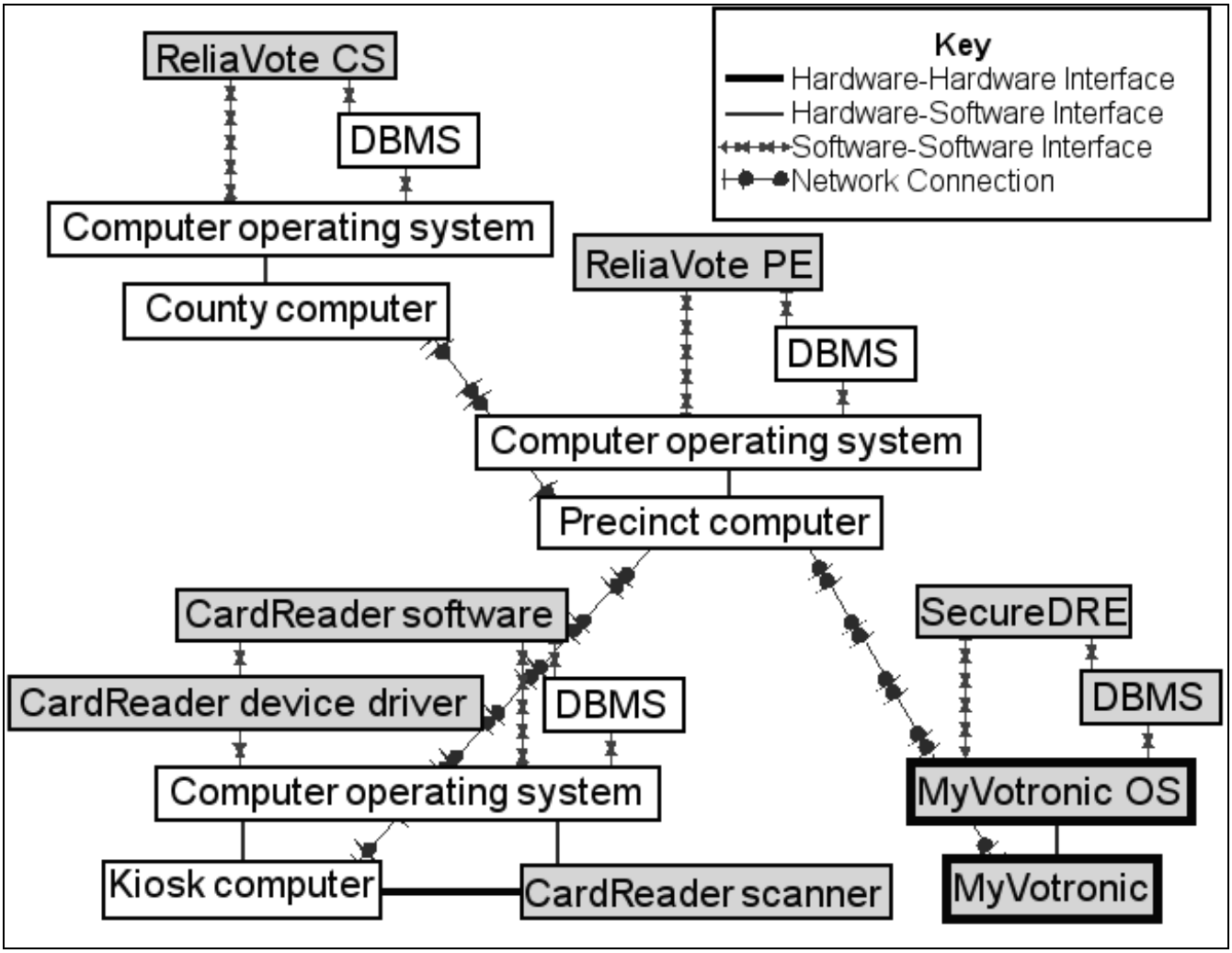
If the dirty data arrive when the Operating System is processing a General User's request for the network adapter, the Operating System assumes that the packets are intended for that General User. The Operating System gives that User permission to deem the packets "clean." The User "cleans" the data by determining if the packets are encrypted with a valid key. The Security Features of SecureDRE [7] and the authentication scheme of precinct-level networks [4] describe what constitutes a valid key. Cleaned data are given the same permissions as a General User.

It should be noted that the Operating System assumes that General Users are trustworthy. In practice, the only General Users that should be using the MyVotronic are the database management system, which does not connect to a network, and SecureDRE, which is a trustworthy software application because it will authenticate data packets from the network.

2.6. Deployment of the Product.

Figure 2 shows the deployment diagram for all InnoVote products and necessary third-party components. Items that this document describes are surrounded with thick boxes.

Figure 2: 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 MyVotronic DRE machine and the SecureDRE software that executes thereon.

3.1.1. System Feature 1: Power on

3.1.1.1. Purpose of Feature

This feature allows the system to receive electrical current from either a direct-current source (such as a battery) or an alternating-current source and convert it to direct current. All other operations of the system require electrical current to perform.

3.1.1.2. Required Hardware Components

The following components of §2.2 are necessary for correct execution of this feature:

- ACPI power supply
- AC adapter or lithium ion battery
- Power on/off button

3.1.2. System Feature 2: Charge battery

3.1.2.1. Purpose of Feature

This feature allows the replaceable battery to charge when the MyVotronic machine is connected to an alternating-current power source. The battery should stop charging when it is completely charged.

3.1.2.2. Required Hardware Components

The following components of §2.2 are necessary for correct execution of this feature:

- ACPI power supply
- AC adapter
- Lithium ion battery

3.1.3. System Feature 3: Perform mathematical and string operations on data

3.1.3.1. Purpose of Feature

This feature allows the system to perform mathematical and text-string operations on data. All operations should be able to be reduced to one or more true-false operations that can then be mapped to an electrical circuit.

Essentially, this feature requires that the system contain at least one processor and a means of sending data and operations to the processor. The feature also requires that MyVotronic OS utilize an efficient process-scheduling algorithm.

3.1.3.2. Required Hardware Components

The following components of §2.2 are necessary for correct execution of this feature:

- ACPI power supply
- AC adapter or lithium ion battery
- System bus
- Microprocessor

3.1.4. System Feature 4: Store data in memory

3.1.4.1. Purpose of Feature

This feature allows the system to store data in temporary memory (RAM) for future processing. It is assumed that the data will originate either from hardware input or from an operation performed by the microprocessor on existing data. This feature is necessary for correct operation of SecureDRE.

This feature requires that MyVotronic OS employ an efficient memory management algorithm.

3.1.4.2. Required Hardware Components

The following components of §2.2 are necessary for correct execution of this feature:

- ACPI power supply
- AC adapter or lithium ion battery
- System bus
- Microprocessor
- RAM

3.1.5. System Feature 5: Retrieve data from memory

3.1.5.1. Purpose of Feature

This feature allows the system to retrieve data from RAM for processing. The feature is necessary for correct operation of SecureDRE.

3.1.5.2. Required Hardware Components

The following components of §2.2 are necessary for correct execution of this feature:

- ACPI power supply
- AC adapter or lithium ion battery
- System bus
- Microprocessor
- RAM

3.1.6. System Feature 6: Accept input from a touchscreen

3.1.6.1. Purpose of Feature

This feature allows the system to accept input from a touchscreen and store it in temporary memory for further manipulation. Numerous software features of the SecureDRE software (reference [6]) require that the machine accept input from a touchscreen and store it.

3.1.6.2. Required Hardware Components

The following components of §2.2 are necessary for correct execution of this feature:

- ACPI power supply
- AC adapter or lithium ion battery
- System bus
- Microprocessor
- RAM
- Display adapter
- Display screen
- Touchscreen

3.1.7. System Feature 7: Accept and display input from a keyboard

3.1.7.1. Purpose of Feature

This feature allows the system to accept input from a keyboard and store it in temporary memory for further manipulation, then display the input on a display in a user-viewable manner. The SecureDRE software operation of casting a vote for a write-in candidate requires the successful operation of this feature.

3.1.7.2. Required Hardware Components

The following components of §2.2 are necessary for correct execution of this feature:

- ACPI power supply
- AC adapter or lithium ion battery
- System bus
- Microprocessor
- RAM
- Modified keyboard
- Display adapter
- Display screen

3.1.8. System Feature 8: Accept input from a network adapter

3.1.8.1. Purpose of Feature

This feature allows the system to accept input from a network adapter and store it in temporary memory for further manipulation. Numerous software operations of SecureDRE require that the MyVotronic accept data from a network adapter and store it for processing.

3.1.8.2. Required Hardware Components

The following components of §2.2 are necessary for correct execution of this feature:

- ACPI power supply
- AC adapter or lithium ion battery
- System bus
- Microprocessor
- RAM
- Network adapter

3.1.9. System Feature 9: Send output to a network adapter

3.1.9.1. Purpose of Feature

This feature allows the system to send output from main memory to a network adapter.

3.1.9.2. Required Hardware Components

The following components of §2.2 are necessary for correct execution of this feature:

- ACPI power supply
- AC adapter or lithium ion battery
- System bus
- Microprocessor
- RAM
- Network adapter

3.1.10. System Feature 10: Accept input from an optical scanner

3.1.10.1. Purpose of Feature

This feature allows the system to accept input from an optical scanner and copy it into memory for processing. The SecureDRE software operation of modifying a printed ballot requires the successful operation of this feature.

3.1.10.2. Required Hardware Components

The following components of §2.2 are necessary for correct execution of this feature:

- ACPI power supply
- AC adapter or lithium ion battery
- System bus
- Microprocessor
- RAM
- Bar code scanner

3.1.11. System Feature 11: Store data on a magnetic disk

3.1.11.1. Purpose of Feature

This feature allows the system to write data to a magnetic disk for storage. It is assumed that the disk will retain its data even when the MyVotronic machine is powered off. This feature is necessary for correct operation of SecureDRE.

3.1.11.2. Required Hardware Components

The following components of §2.2 are necessary for correct execution of this feature:

- ACPI power supply
- AC adapter or lithium ion battery
- System bus
- Microprocessor
- RAM
- DMA module and controller
- IDE controller
- Hard disk

3.1.12. System Feature 12: Retrieve data from a magnetic disk

3.1.12.1. Purpose of Feature

This feature allows the system to retrieve data from a magnetic storage disk and copy it into a memory buffer for processing. Numerous software operations of SecureDRE require the successful execution of this feature.

This feature requires that MyVotronic OS employ an efficient disk-reading algorithm.

3.1.12.2. Required Hardware Components

The following components of §2.2 are necessary for correct execution of this feature:

- ACPI power supply
- AC adapter or lithium ion battery
- System bus
- Microprocessor
- RAM
- DMA module and controller
- IDE controller
- Hard disk

3.1.13. System Feature 13: Delete data from a magnetic disk

3.1.13.1. Purpose of Feature

This feature allows the system to make data stored on a magnetic storage disk inaccessible to high-level software operations. This operation does not physically remove the data from the disk, but places an indicator on the disk immediately before the data that indicates that it is "deleted". The data can still be recovered until overwritten. Numerous software operations of SecureDRE require the successful execution of this feature.

3.1.13.2. Required Hardware Components

The following components of §2.2 are necessary for correct execution of this feature:

- ACPI power supply
- AC adapter or lithium ion battery
- System bus
- Microprocessor
- RAM
- DMA module and controller
- IDE controller
- Hard disk

3.1.14. System Feature 14: Physically erase data from a magnetic disk

3.1.14.1. Purpose of Feature

This feature allows the system to physically erase data from a magnetic disk or "format" some part of the disk. With most existing magnetic disks, repeated execution of this operation will make recovery of the data extremely difficult.

3.1.14.2. Required Hardware Components

The following components of §2.2 are necessary for correct execution of this feature:

- ACPI power supply
- AC adapter or lithium ion battery
- System bus
- Microprocessor
- RAM
- DMA module and controller
- IDE controller
- Hard disk

3.1.15. System Feature 15: Send output to a screen

3.1.15.1. Purpose of Feature

This feature allows the system to send data to a video adapter for displaying it on a screen. The feature is necessary for correct operation of the SecureDRE software.

3.1.15.2. Required Hardware Components

The following components of §2.2 are necessary for correct execution of this feature:

- ACPI power supply
- AC adapter or lithium ion battery
- System bus
- Microprocessor
- RAM
- Display adapter
- Display screen

3.1.16. System Feature 16: Send output to a printer

3.1.16.1. Purpose of Feature

This feature allows the system to send data to a printer for printing on paper. The SecureDRE software operation of printing a ballot requires the successful operation of this feature.

This operation needs to be interrupt-driven. Its use will be to print a ballot, a SecureDRE function that is of great practical importance in an election. Despite the inherent slowness of a printer as compared to a processor, the system needs to halt all other operations until the paper ballot has finished printing.

3.1.16.2. Required Hardware Components

The following components of §2.2 are necessary for correct execution of this feature:

- ACPI power supply
- AC adapter or lithium ion battery
- System bus
- Microprocessor
- RAM
- Printer port and printer

3.1.17. System Feature 17: Regulate temperature of hardware components

3.1.17.1. Purpose of Feature

This feature allows the system to detect the temperature of hardware components and cool the system as necessary by operating the fan or other cooling device.

3.1.17.2. Required Hardware Components

The following components of §2.2 are necessary for correct execution of this feature:

- ACPI power supply
- AC adapter or lithium ion battery
- Cooling fan
- Thermal sensor

3.1.18. System Feature 18: Maintain status of battery

3.1.18.1. Purpose of Feature

This feature allows the system to maintain the status of the battery used for powering the machine. The system must be able to detect the charge level of the battery when it is being used as the primary power source as well as the condition of the battery when the system is using AC power.

3.1.18.2. Required Hardware Components

The following components of §2.2 are necessary for correct execution of this feature:

- ACPI power supply
- AC adapter (when battery is not source of power)
- Lithium ion battery
- Microprocessor
- System bus
- RAM

3.1.19. System Feature 19: Display status of battery

3.1.19.1. Purpose of Feature

This feature allows the system to display the status of the battery when it is either not able to charge or has extremely low power.

3.1.19.2. Required Hardware Components

The following components of §2.2 are necessary for correct execution of this feature:

- ACPI power supply
- AC adapter (when battery is not source of power)
- Lithium ion battery
- Microprocessor
- System bus
- RAM
- Display adapter
- Display screen

3.1.20. System Feature 20: Emergency backup

3.1.20.1. Purpose of Feature

This feature allows the system to perform an emergency save of the current contents of volatile memory (RAM) to the hard disk when the battery is very low on power, not present, or not able to charge. When the battery is the source of power and is low on power, the system powers down after successfully writing the data to disk.

3.1.20.2. Required Hardware Components

The following components of §2.2 are necessary for correct execution of this feature:

- ACPI power supply
- AC adapter (when battery is not source of power)
- Lithium ion battery
- Microprocessor
- System bus
- RAM
- DMA module and controller
- IDE controller
- Hard disk

3.1.21. System Feature 21: Maintain internal time

3.1.21.1. Purpose of Feature

This feature allows the system to maintain an internal time from which it will derive and synchronize software-based clocks. Numerous software operations of SecureDRE require the successful execution of this feature.

3.1.21.2. Required Hardware Components

The following components of §2.2 are necessary for correct execution of this feature:

- CMOS battery
- CMOS system clock
- System timer

3.1.22. System Feature 22: Power off

3.1.22.1. Purpose of Feature

This feature allows the system to shut off all hardware operations except for System Feature 2, “Charge battery.”

3.1.22.2. Required Hardware Components

The following components of §2.2 are necessary for correct execution of this feature:

- ACPI power supply
- AC adapter or lithium ion battery
- Power on/off button

3.2. Performance Requirements.

The features described in this section are requirements that are necessary for MyVotronic to operate in a reasonable amount of time or under normal conditions.

3.2.1. Performance Requirement 1: Process data quickly

Most operations of MyVotronic require the use of a microprocessor to manipulate data. Because of the data-intensive nature of a voting machine's operations, the processor must be able to process data very rapidly. The designer's vision of the MyVotronic is a single-processor machine; however, the design could be adapted to a multiprocessor model. If the MyVotronic is implemented as a uniprocessor, the designer suggests that the processor speed be at least 2.5 GHz (2.5 billion operations per second).

3.2.2. Performance Requirement 2: Store and retrieve data quickly

Many operations of MyVotronic require that data be stored (written) and retrieved (read) from various media. Most storages and retrievals will be from the RAM or main memory; however, data will also be stored on the hard disk. As with Performance Requirement 1, the data-intensive nature of the MyVotronic's operations necessitate that all data operations involving the RAM and the hard disk be performed rapidly.

3.2.3. Performance Requirement 3: Function in broad temperature range

The MyVotronic needs to operate correctly in a broad temperature range. It cannot be assumed that the machine will always operate in conditioned locations; therefore, it needs to operate correctly when the surrounding air temperature is in the range of –40 to +125 degrees Fahrenheit.

3.2.4. Performance Requirement 4: Operate on battery power long enough to complete election

In the event of a power failure during an election, the MyVotronic's battery must, when fully charged, be able to sustain power for at least 12 hours before it must perform System Feature 20, "Emergency backup." This requirement assumes intense use of hardware components, as would be expected during certain elections.

3.2.5. Performance Requirement 5: Recharge battery in 24 hours or less

When connected to a steady source of AC power, the system must be able to recharge a battery from the fully discharged state to fully charged. This requirement assumes that the battery is "good" and able to hold a charge.