

Context Description: Posted Dec. 1, 2006

This draft report was prepared by NIST staff at the request of the Technical Guidelines Development Committee (TGDC) to serve as a point of discussion at the Dec. 4-5 meeting of the TGDC. Prepared in conjunction with members of a TGDC subcommittee, the report is a discussion draft and does not represent a consensus view or recommendation from either NIST or the TGDC. It reflects the conclusions of NIST research staff for purposes of discussion. The TGDC is an advisory group to the Election Assistance Commission, which produces voluntary voting system guidelines and was established by the Help America Vote Act. NIST serves as a technical advisor to the TGDC.

The NIST research and the draft report's conclusions are based on interviews and discussions with election officials, voting system vendors, computer scientists, and other experts in the field, as well as a literature search and the technical expertise of its authors. It is intended to help in developing guidelines for the next generation of electronic voting machine to ensure that these systems are as reliable, accurate, and secure as possible. Issues of certification or decertification of voting systems currently in place are outside the scope of this document and of the TGDC's deliberations.

VOTING MACHINES: RELIABILITY REQUIREMENTS, METRICS, AND CERTIFICATION

**Maximilian M. Etschmaier
September 2006**

This report is submitted by GME International Corporation as deliverable for task 6 of contract SB134105Z0023 through KT Consulting, Inc.

Foreword

In the 158-page text of the Voluntary Voting System Guidelines of 2005 (VVSG2005) the following section is the only explicitly identified requirement on the reliability of voting machines:

“The reliability of voting systems devices shall be measured as Mean Time Between Failure (MTBF) for the system submitted for testing. MTBF is defined as the value of the ratio of operating time to the number of failures that have occurred in the specified time interval. A typical system operations scenario consists of approximately 45 hours of equipment operations, consisting of 30 hours of equipment set-up and readiness testing and 15 hours of election operations. For the purpose of demonstrating compliance with this requirement, a failure is defined as any event which results in either the:

- *Loss of one or more functions*
- *Degradation of performance such that the device is unable to perform its intended function for longer than 10 seconds.*

The MTBF demonstrated during certification testing shall be at least 163 hours.”

[Section 4.3.3, page 85]

Our charge for this present work is to:

- *“Investigate the continued suitability of using the MTBF as the sole measure of voting system reliability.*
- *Recommend that either the MTBF be retained as the sole measure of reliability, or be replaced or enhanced by other metrics or techniques.”*

The results of our work are summarized in the three papers that comprise this report.

We have approached the question as we would approach any problem:

- We examined the concept of reliability and determined what it means in the context of voting machines.
- We determined what should be the object of analysis, and found that it is the voting machine that can realistically be subjected to reliability requirements; and that beyond that, for the precinct level voting system, a requirement for voting machine availability should be established.
- We determined what should be expected of a voting machine in terms of system performance.
- We analyzed if and how the performance requirements can be met.

- We defined what regulatory process and procedures would be necessary to successfully implement the performance requirements and lead to deployment of voting machines that will meet the requirements.

Our approach and our results differ from those underlying VVSG2005.

- We regard statistical analysis as only one way to extract information about the system reliability. To the extent they are practical, other methods, such as logical analysis of causal relationships, analysis following established laws of nature, and mathematical modeling and simulation, may yield more reliable information. Our analysis, therefore, primarily rests on a logical analysis of system functions, and uses statistical analysis only as a means of validation. The disadvantage of using statistical methods as the primary source of information about system performance comes from the fact that even moderately complex processes may have a large variance. Inordinate amounts of testing is then required before certain combinations of failures (e.g., “malicious code”) will be encountered; some failures, such as certain purposely hidden functionality may be impossible to identify through testing, while they might be identified easily through direct analysis.
- VVSG2005 treats reliability and accuracy as independent characteristics of a system. We see accuracy and reliability as tightly interconnected. Accuracy is a system characteristic that is determined by many independent processes. Some inaccuracy is caused by failures of system components involved in manipulating the information. Other inaccuracy may be inherent in a process, such as optical information recognition, although ultimately, any inaccuracy may also be viewed as a failure or the consequence of one. In the framework of our analysis, accuracy requirements are applied to interfaces between media, such as the human-machine interface, or optical character recognition, rather than for the overall system as an “end-to-end” requirement.
- VVSG2005 calls for testing labs to independently determine system performance, such as reliability. The testing labs, while paid by the vendor, work under the authority of the EAC. We believe that this arrangement may lead to considerable misunderstanding of responsibility for the in-service performance of voting machines. We propose, therefore, that system performance be determined through analysis of the system by the vendor, augmented by analysis and testing by a qualified testing lab. Any lab would work for the vendor, and it would remain the vendor’s responsibility that the voting machine meet the performance requirements upon delivery, and continue to do so during its service life. The certifying authority would check the documentation submitted by the vendor, and might perform separate validation tests. Through a performance

monitoring system it would assure that the system continues to perform as required, mandating corrective actions if variances are detected.

Our analysis has identified a path to get voting machines out of the current state where failures and inaccuracies are so frequent that the confidence in the integrity of the electoral system is jeopardized. If this path is followed, failures of voting machines on Election Day and questions about the accuracy will be all but unheard of. Our analysis also separates the issue of voting machine reliability from issues of election management. It can introduce a measure of objectivity into the current debate concerning the election process, and will leave the manufacturers of voting machines with a responsibility that is defined clearly enough so they can meet it.

Our example is civil aviation, where a similar approach is permitting operation of the entire airliner fleet of the country for years without a single catastrophic accident due to aircraft failures. Our example is also the standard for gambling machines in the State of Nevada that, for a system that is quite similar to voting machines in terms of technology and complexity, stipulates requirements that are quite similar to what our analysis is leading to. We believe that it is not unreasonable to expect that the process of counting votes in an election should be conducted at least with the reliability that is achieved in a gambling house.

Contents

Part 1: Critical Issues for Formulating Reliability Requirements

Part 2: Definition of Requirements, Metrics, and the Certification Process

VOTING MACHINES: RELIABILITY REQUIREMENTS, METRICS, AND CERTIFICATION

Part 1

Critical Issues for Formulating Reliability Requirements

Maximilian M. Etschmaier
August 22, 2006

Abstract

During the public comment period for VVSG2005 as well as subsequent to the adoption of the guidelines, questions have been raised if the reliability requirements spelled out in the guidelines are sufficiently stringent, and if the metrics promulgated by the guidelines will lead to the most cost-effective voting systems.

This paper is intended to lay the groundwork for the development of improved reliability requirements and defines how they fit into the overall framework of voting machine design, operation, certification, and procurement. It also shows the relationship between requirements for reliability and other elements of VVSG. It is hoped that this will give rise to a thorough discussion within the entire team working on VVSG2007, which should lead to a consensus on the overall integration of the effort.

The analysis shows an opportunity to more closely tailor reliability requirements to the special, intermittent operational pattern of voting machines. Measures other than the currently used MTBF are suggested that could be more easily complied with, and lead to better performing voting machines.

1. Introduction

Current reliability requirements for voting systems are defined in the Voluntary Voting System Guidelines (VVSG2005), adopted on December 13, 2005 by the US Election Assistance Commission (EAC). During the public comment period, as well as subsequent to the adoption of the guidelines, questions have been raised if the performance targets spelled out in the guidelines are sufficiently stringent, and if the metrics promulgated by the guidelines will lead to the most cost-effective voting systems. E.g., Ronald Crane claims that “*the reliability standard ... permits ... unacceptably high failure rates.*” [VVSG Comments of Ronald E. Crane, 9/21/2005]. Stanley A. Klein calls the requirement for a mean time between failures of only 163 hours “*pathetically low*” [Stanley A. Klein Statement to EAC on Draft VVSG, September 24, 2005].

The reliability requirements of the existing guidelines [VVSG Section 4.3.3] do not provide a clear definition of what constitutes a failure (“*loss of one or more functions, degradation of performance...*”). They appear focused on the rate of failures of the voting machine and its components. While a reliability mandate expressed in terms of a guaranteed time between failures (MTBF) is consistent with practices in reliability engineering, there may be alternative ways that can assure the availability of the functions required of a voting system with greater probability and at a lower cost. These alternatives would start with an analysis of the functions required, and determine the failures that can lead to a loss of these functions. Certification would involve a determination that the loss of “critical” functions can be avoided altogether, except in extremely rare situations.

In this paper we identify the key issues that need to be resolved in order to shape regulation of voting system reliability. We will lay out the options that may exist, cite precedents of how these issues have been dealt with in the past, and outline the choices that have to be made. The intention is to shape a robust consensus that will support whatever regulation is adopted, a prerequisite for any successful regulation.

2. System Reliability Defined

Reliability is a concept that is widely used in a variety of contexts. Although the basic notion is intuitively quite clear, different contexts emphasize different aspects of the concept.

The discipline of Reliability Theory applies mathematical tools of probability theory to derive probabilities and other system performance measures for multitudes of combinations of components with a variety of failure characteristics. It has been very successful in helping design telecommunications and other “physical” systems. However, efforts to extend the tools of Probability Theory to more complex systems, especially those involving human interaction, reveal two problems: analytical problem formulations and solutions become increasingly elusive; and properly framing the problem begins to dominate the effort.

According to [MIL-HDBK-338B, page 4-1], “[t]he traditional, narrow definition of reliability is ‘the probability that an item can perform its intended function for a specified interval under stated conditions.’” It continues, “this narrow definition is applicable largely to items which have simple missions... For large complex systems... it is more important to use more sophisticated concepts such as ‘system effectiveness’ to describe the worth of a system.”

Blanchard and Fabrycky in their book, *Systems Engineering and Analysis* (1981, page 323), emphasize that reliability analysis cannot solely be focused on obtaining measures, but more importantly, needs to consider the purpose of the system and its environment in order to be able to define what are meaningful measures.

“Reliability can be defined simply as the probability that a system or product will perform in a satisfactory manner for a given period of time when used under specified operating conditions. This definition stresses the elements of probability, satisfactory performance, time, and specifying operating conditions. These four elements are very important, since each plays a significant role in determining system/product reliability.”

We shall expand on this by adding that the reliability of a system is determined by its components (“component reliability”) and the interaction among the components (“system integration”); and that operating conditions include the maintenance and logistics support system in place.

It is this expansive definition that is most useful for determining reliability requirements for voting machines and voting systems. Loosely following this definition we will divide the analysis into the following subjects:

1. What is a proper definition of “voting system” that can be subjected to a meaningful reliability analysis?
2. What functions are required of the voting system, and how important is each one of the functions?
3. What is the operating environment, including operational (usage) patterns, the maintenance process, and the logistics support system for the voting systems?

Examining the differences between voting systems and other types of systems will help identify the extent to which standard industry practices can be adopted.

2.1. What System

In general, any object can be viewed as an element of a multitude of systems, and any system is an element of other systems. A careful definition of the system that is subject of analysis is a prerequisite to any successful analysis.

The term “voting system” is generally used to refer to several different levels of systems. At the lowest level is the voting machine, the product that is procured from a “vendor.” A voting machine is rarely used in isolation, but usually deployed together with other machines at a polling station (“precinct”). Even if these machines are not physically linked (such as through a common power supply, or because they all transmit information to the same terminal), they together form a system in a functional (logistical) sense. It is jointly that they serve the voters assigned to the precinct. And if one machine should fail, the rest of them need to take up the slack. To the extent that failed machines are repaired or replaced, they also share the same repair capacity and spare parts pool.

The precinct voting systems may in turn be linked to regional voting systems, either through telecommunication or logistically. However, unless an entire regional system is procured from a single vendor (or prime contractor), defining reliability requirements for a regional system does not appear to be an issue that needs to be addressed in the reliability requirements of the VVSG. Instead, it will probably be covered through requirements for telecommunication systems and logistics requirements that directly scale up from those for precinct level systems.

The current guidelines require specifying reliability requirements at the voting machine as well as the precinct level.

E.g., Section 4.1.1, Accuracy Requirements, of VVSG2005 specifies maximum error rates at the “*DRE voting system,*” the “*precinct-count voting system,*” and the “*central-count system.*”

The mandate of Section 2.1.4, Integrity, that “*all systems shall ... [p]rotect against a single point of failure that would prevent further voting at the polling place*” explicitly requires an examination of failures of the precinct-level voting system.

However, the section of VVSG2005 that explicitly deals with reliability requirements [Section 4.3.3, Reliability] appears to define them strictly in terms of the voting machine when it requires that “*the reliability of voting systems shall be measured ... for the system submitted for testing.*”

Some further examination is required of the composition of voting machines. Figure 1 shows a schematic model of a typical voting machine of current vintage. A display, possibly interactive, and a number of electronic components are imbedded in a structure of mechanical and electromechanical components. In a “physical” sense, all these are connected and require each other to function properly. Increasingly, though, the way they function is determined by software. The software, which often includes “firmware,” can be implemented directly in the electronic components, or be made available through telecommunication systems. It is the software then that ultimately determines the way the system functions. If failures are defined as “*a loss of one or more functions,*” [VVSG2005, Section 4.3.3, Reliability] software, in its composition as well as the mode in which it is implemented (or delivered) thus is a central element of any reliability analysis and specification of reliability requirements.

VOTING MACHINE SYSTEM COMPONENTS

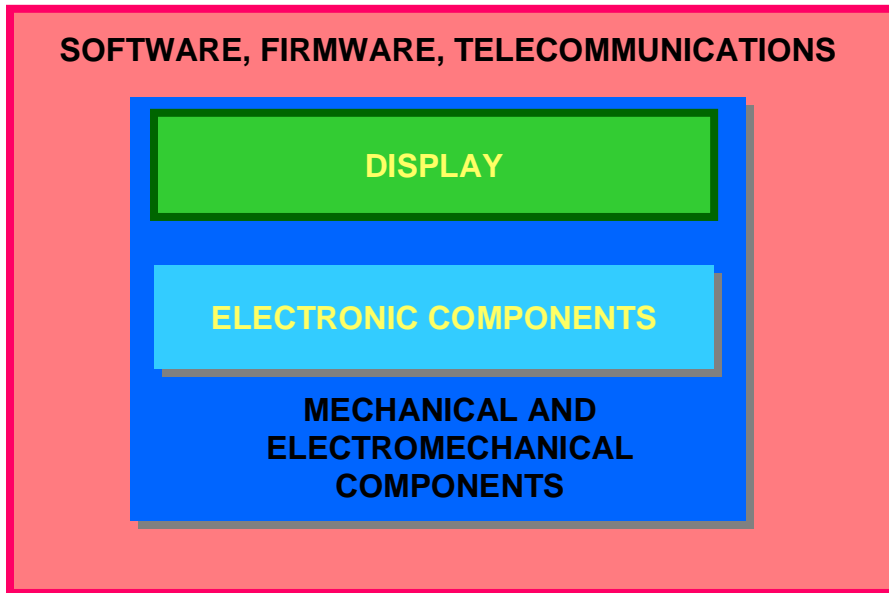


Figure 1

We recommend therefore, that the functionality of software be an integral part of reliability requirements. Also included should be ways in which the software can change or be changed during operations, and transparency requirements for software. Separate from this may be issues like programming style and robustness of programs.

This recommendation follows directly from the Help America Vote Act (HAVA Section 301, VVSG I, PAGE 9) which defines a voting system as the “[t]otal combination of mechanical, electromechanical, or electronic equipment (including the software, firmware, and documentation required to program, control, and support the equipment)...”

VVSG2005 Section 4.3.3, Reliability, makes no distinction between hardware and software when it defines a failure as “any event which results in either the loss of one or more functions [or] degradation of performance...” Also, the reliability requirement included in Section 4.1.1, Accuracy Requirements, largely refer to functions that in current and future voting systems are performed by software.

2.2. System Functions

Complex systems typically include the capability to perform numerous functions. Not all of these are equally important. Some of them may be “critical” for the use to which the system is put, others carry less grave consequences if they are lost, and yet others,

especially in systems using off the shelf standard components, are not needed at all. We shall discuss later what “critical” means of a function.

A prerequisite for specifying reliability requirements for a system is that all needed functions are identified and the level of criticality determined for each. Voting system functions are identified in the Help America Vote Act, and in various places of the VVSG2005. Help America Vote Act (HAVA Section 301, VVSG I, PAGE 9) lists the functions as

- *“define ballots*
- *cast and count votes*
- *report or display election results*
- *maintain and produce any audit trail information.”*

It also defines certain “*practices and associated documentation...*” as part of the voting system.

HAVA SEC. 301 further defines as “*voting systems standards*” functions that “*permit the voter to verify ... the votes selected ... before the ballot is cast and counted; provide the voter with the opportunity ... to change the ballot or correct any error before the ballot is cast and counted; ...notify the voter [if he or she] ... has selected more than one candidate for a single office on the ballot; notify the voter ... of the effect of casting multiple votes for the office; [and] provide the voter with the opportunity to correct the ballot before the ballot is cast and counted.*”

Further functions of voting systems are identified and specified throughout VVSG2005.

Figure 2 provides a generic overview of functions of a voting system compiled from these and other sources.

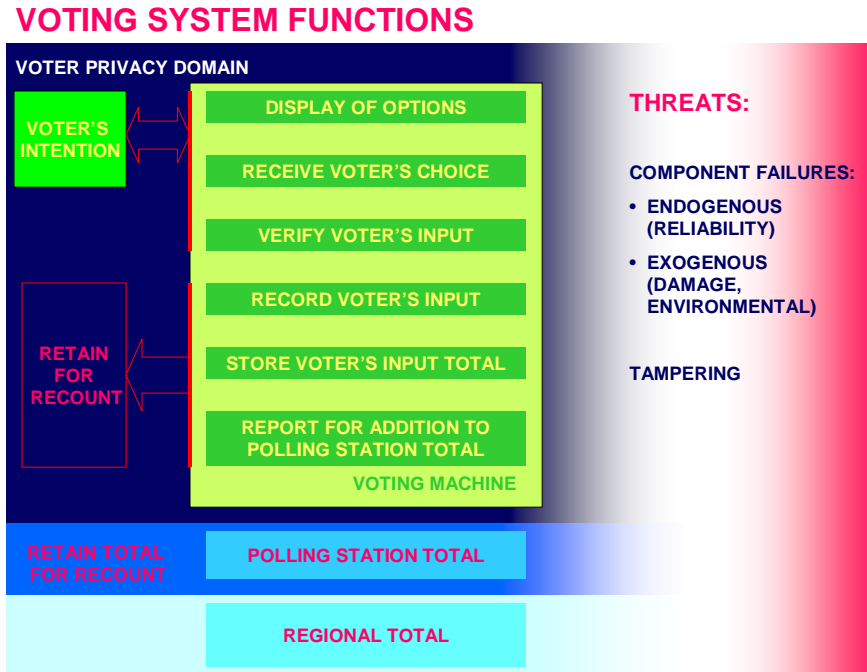


Figure 2

In some form the voting system presents to the voter the ballot, which specifies the choices available. The system receives the voter's choices, and after verifying those, records them. The system will store the voter's input, accumulate totals, and report those as input to the precinct totals. The system will also retain the voter's input and the station total for possible recounts. Throughout this entire process the privacy of the voter must be protected.

In order to preserve the integrity of the system, some or all of these functions may be duplicated in a manner that establishes a maximum of trust in the results.

At the precinct level, the totals from all machines are accumulated, stored for a possible recount, and transmitted to be included in the regional total.

Availability of these functions can be threatened by component (including software) failures, and by tampering. Component failures may be endogenous, i.e., the result of inherent component reliability, or they may be inflicted from the outside, either by damage or by exposure to environmental conditions outside of what the system is designed for.

As indicated above, a key prerequisite for specifying reliability requirements is to classify potential failures, in particular identifying those that are "critical." This requires that we define what is meant by "critical."

In aviation a failure is “critical” if it poses a threat to human life. Human life is considered so important that, at least to the extent it is humanly and scientifically possible to anticipate them, failures that threaten it have to be avoided at all cost. A system in which the possibility of critical failures occurring cannot be excluded is considered unfit for the purpose of civil aviation. The rigor with which this criterion is applied has greatly improved aviation safety and turned an inherently unsafe mode of transportation into one of the safest. The rigor of analysis is also responsible for the fact that this was accomplished without increasing overall cost. [Etschmaier 1984, Nowlan 1978] There is little reason to doubt that the record of aviation cannot be duplicated elsewhere.

What then would “critical” mean in voting systems? Would the loss or alteration of one vote be so damaging that it has to be avoided at all cost? What *is* the harm from the loss of one vote? The answer is by no means trivial. It is clear that loss or alteration of one vote might be decisive for the outcome of an election. If it would not be one vote, then maybe two, or three, ... A study by the Brennan Center [The Machinery Of Democracy: Protecting Elections In An Electronic World, The Brennan Center Task Force On Voting System Security, 2006] shows how small differences in vote count can change the outcome of an election. Potentially at least, that might mean a difference between war and peace, possibly jeopardizing many more lives than can be affected by the crash of an airliner. However, public opinion, as well as the legal system may not support this analogy.

The Help America Vote Act and VVASG2005 define a range of functional capabilities that are required of voting systems, as well as functions that are required to assure that the consequences of failures are tolerable. But they do not define a tolerance limit for those later functions.

Some examples:

“vi. Voting system design shall ensure that erroneous responses (to error messages) will not lead to irreversible error.” [Section 2.1.5.1]

“... each piece of voting equipment that tabulates ballots shall provide a counter that ... d. Prevents or disables the resetting of the counter by any person other than authorized persons at authorized points” [Section 2.1.8]

“e. In the event of a failure of the main power supply external to the voting system, provide the capability for any voter who is voting at the time to complete casting a ballot, allow for the successful shutdown of the voting system without loss or degradation of the voting and audit data, and allow voters to resume voting once the voting system has reverted to back-up power” [Section 2.3.3.1]

“Recovery from a non-catastrophic failure of a device requires restoration of the device to the operating condition existing immediately prior to the failure without loss or corruption of voting data previously stored” [Section 2.1.3]

“f. Provide the capability for voters to continue casting ballots in the event of a failure of a telecommunications connection within the polling place or between the polling place and any other location.” [Section 2.3.3.1]

If it is determined that “critical” failures have to be avoided at all cost, then, by definition, voting systems that are designed in such a way that the occurrence of critical failures cannot be excluded, are not considered fit for the purpose, and can not receive certification. If on the other hand critical failures are permitted to happen, then determination of acceptable rates will depend on economic calculus. The unavoidable next step would be to determine the cost of a “critical” failure.

A thorough debate would be desirable to form a consensus on this issue.

The experience of civil aviation shows that determining optimal system reliability is a many dimensional problem, and reducing it to the traditional model of economic optimization where increasing investment increases system reliability, and increasing system reliability decreases system operating cost may reduce it to a subspace that does not contain the optimum.

Irrespective of how the consequences of failures are determined, Figure 3 presents an overview of what generically might constitute “critical” failures.

CRITICAL FAILURES OF VOTING SYSTEM

- FAULTY DISPLAY OF OPTIONS
- UNCERTAINTY IF VOTER'S CHOICE HAS BEEN RECORDED
- FALSE RECORDING OF VOTE CAST
- CHANGE OF STORED VOTES
- FALSE TRANSMISSION FOR POLLING STATION TOTALS
- INJURY TO VOTERS OR STAFF

- PROVIDE OPENING FOR TAMPERING
- VIOLATION OF VOTER PRIVACY

- FALSE ACCUMULATION OF POLLING STATION TOTALS
- FALSE TRANSMISSION FOR REGIONAL TOTALS
- INSUFFICIENT NUMBER OF OPERATIONAL MACHINES AT POLLING STATION

- APPEARANCE OF IRREGULARITY

Figure 3

The failures are listed in an order that roughly reflects the transition from the voting machine level to the level of the regional voting system.

Faulty display of options might limit the choices the voter is presented with and thus might deny the voter his/her choice.

Uncertainty if a voter's choice has been recorded might lead to a quandary. The vote might be lost or the voter would vote twice, either of which would not be acceptable.

If a voting system is designed in such a way that votes cast may be recorded wrongly, or at some later time changed either inadvertently or intentionally, or that voting machine totals are transmitted for precinct totals different from what is recorded, it does not meet the most basic requirements.

The design of a voting machine should be expected not to be such that a failure would expose voters or staff to injury.

Tampering is intentional manipulation of information stored in a voting machine or system. The failure of the voting system is not the tampering itself, but the fact that the system provided an opening for it. Protection against tampering could be in the form of a physical barrier, or it could be in the form of security arrangements. In the latter case, the security arrangements would have to be regarded as integral parts of the voting system and be included in a specification of reliability requirements.

Voter privacy is mandated by the Help America Vote Act. There appear to be many opportunities for violation, some intentional and abusive, but many inadvertent. It may be questionable if all these violations should be regarded as equally "critical" system failures. However, it might be difficult to draw a line and stop possibilities for inadvertent violations turning into intentional ones. In the absence of any clear differentiation it may be best to consider all opportunities as equally critical.

False accumulation of polling station totals and false transmission of precinct totals for inclusion in regional totals are the regional system equivalent to what was discussed above for the precinct level.

The law requires that all voters be given access to vote. If a precinct can not accept votes because there are no or an insufficient number of voting machines available (i.e., in a serviceable condition) then voters are denied the opportunity to vote, a system failure as "critical" as all the other "critical" failures mentioned here. Protection against this type of failure can occur by either determining the number of voting machines assigned to a precinct in such a way that, given a failure rate of individual machines, a situation can not occur (i.e., has an infinitesimally small probability of occurring) where there is an insufficient number of operational machines at the precinct. Alternatively, provisions can be made to have sufficient spare machines available and the required logistics system in place such that failed machines are replaced before the number of unserviceable

machines can reach a critical value. In the second case, the availability of spare machines and the logistics system in place need to be part of determination of the reliability requirement.

A critical aspect of a voting system is the confidence in the result it provides the public. While the failures discussed so far are considered “critical” because they directly affect the outcome of an election, there are situations where the outcome is not actually affected, but there is significant doubt of the integrity of the process – an appearance of irregularity. There are numerous examples where doubts about the regularity of an election have caused more damage than the miscounting of a few votes. Any opening that a system provides for the appearance of irregularity therefore has to be viewed as a “critical” failure.

3. System Operations

System operations are where the system with its functional capabilities is deployed for purposeful use – the *raison d’être* of the system. It would seem then that this subject should be discussed before discussing the delineation of a voting system and the identification of its functions. In reality, these three subjects are closely interrelated. Designing a system involves a circular process of iteration between them. The same is true for defining reliability requirements.

The information that defines system operations can be assembled in what might be called a statement of mission for the system. Such a statement includes what the system is expected to accomplish, the patterns of usage the system is subjected to, the general environmental conditions the system is exposed to, and costs and benefits associated with system operations and system failures. We shall focus here on what appears relevant to determining how system reliability requirements can be formulated.

What the system is expected to accomplish, has largely been covered with the system functions. In summary it can be stated as follows:

- Assure availability of correct voting options to every voter
- Record every vote without ambiguity and accurately add to machine total
- Accurately report machine total for inclusion in polling place total
- Assure privacy of every voter
- Exclude possibility of tampering
- And assure the performance of this with economy and efficiency, and without the appearance of impropriety.

Figure 4 provides an overview of the patterns of usage the system is subjected to.

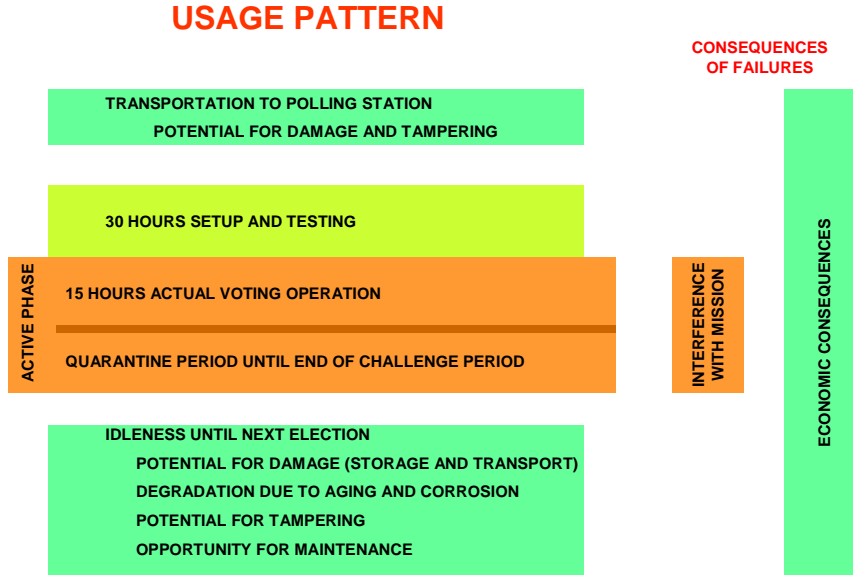


Figure 4

A voting machine is in active use only for a short time, during an election, and is in a state of secure readiness for the period after the election during which recounts are possible. According to Section 4.3.3, Reliability, in VVSG 2005, voting operations last about 15 hours. The “active phase” is preceded by a period of set-up and testing, which may take as much as 30 hours. Prior to that, the voting machines are shipped from the storage facility to the polling station.

It is only during the active phase that the voting machine is performing its core mission, and failures that could interfere directly with the performance of the mission can only occur during that period. Outside the active phase, the voting machine is exposed to possible failures resulting from damage, and degradation. If the voting machines are checked out properly prior to each election, the consequences of these failures are purely economic. The failures would not constitute “critical” failures.

Storage might also provide opportunities for tampering, which might be difficult to detect on checkout. Opening the voting machine to this possibility would constitute a “critical” failure [See e.g., *The Machinery of Democracy: Protecting Elections in an Electronic World*, The Brennan Center Task Force on Voting System Security, 2006]. Certain protection against this could be included in the design/reliability requirements. Much of it, though, will need to be provided through security measures. However, although they need to be considered in defining reliability requirements, they will in general not be within the responsibility of the voting machine vendor.

There is also the possibility that a failure outside of the active phase might cause serious injury to people handling voting machines. These would be “critical” failures. However, they would not infringe on the core mission of a voting machine.

In summary, the possibility of “critical” failures outside the active phase appears limited, and those that can occur might be outside the scope of what is required of a vendor.

The general environmental conditions the system is exposed to are not any more demanding than those of common office machinery and many consumer products, including consumer electronics.

Costs and benefits associated with system operations and system failures are significant aspects of the operational environment. They will be examined in a separate paper.

4. Voting Systems in Perspective

To the extent that it is possible, reliability guidelines for voting systems will emulate practices already in place for other types of machinery. In addition to expediency, this may protect the endeavor against costly mistakes. However, equally costly mistakes can be made by adopting practices from essentially different environments. A closer examination of how voting machines compare with other machinery is therefore in order.

In principle, voting machines are very simple systems, adding votes into registers and retaining an audit trail for verification of results. Although accuracy is of the essence, speed is not, and the volume of information that needs to be stored is quite modest. They only need to work for 15 hours at a time, after which there is a long idle period during which any amount of testing and maintenance can easily be accommodated.

Voting machines are sold and used in relatively large numbers. Access to them is limited by law and regulation. The personnel maintaining them are, or at least can be required to possess defined skills and meet defined security requirements. It should, therefore, be possible to all but rule out abuse through unqualified staff.

Many office machines and consumer products perform tasks that are significantly more complex. There are only three major issues that complicate matters for voting machines:

- The requirement for privacy means that the operation of a voting machine cannot be externally monitored as voting occurs. Verification of proper operation, therefore, complicates the design as well as operation and maintenance during the active phase.
- Design and operation of voting machines is governed by legal and regulatory requirements.
- Voting machines are procured under government procedures that define the relationship between the vendor and the user, and limit the amount of collaboration between the two.

5. Strategies for specifying reliability requirements

Assuming that “critical” failures outside the active phase do not need to be considered in reliability requirements imposed on a vendor of voting machines, two strategies emerge. Requirements for precinct level and regional voting systems are separate from these.

Strategy 1: Require that the voting machines be designed in such a way that “no” failures of any kind will occur during an active phase. Since in general the possibility of failures cannot be excluded entirely, “no failures” is interpreted as a very (or extremely) small probability of a failure.

In general, there is no relationship between the longevity of a system and the failure probability during a very small, initial period. It would therefore suffice to demonstrate that the failure probability during a specified number of active phases would not exceed the limit. Checks could be specified that would verify the condition of a machine before each active phase.

If the failure rate increases with age, periodic “reconditioning” or “overhauls” might be prescribed, as might be a limit on the overall service life. “Reconditioning” or “overhaul” might also be prescribed instead of the checks mentioned above before each active phase to make sure that the failure process will always start at the same point. However, such a strategy may run afoul of the phenomenon of “infant” mortality where the failure rate of a new (or “like new”) system is significantly higher than that of one that has been operating for some time, i.e., has been “burned in.”

The metric currently prescribed, the MTBF, can be used as a proxy for the failure probability during an active phase. However, that would be meaningful only under the condition that the failure rate is non-decreasing. Given the intermittent operational pattern, though, even in this situation, other measures, especially direct probability statements, are more readily understood and easier to measure.

A prerequisite for strategy 1 is that the voting machine is a self-contained “black box” that is not opened during active phase. This may not be an unreasonable expectation since many consumer goods and electronics systems are already designed that way.

The most important aspects of Strategy 1 are summarized graphically in Figure 5.

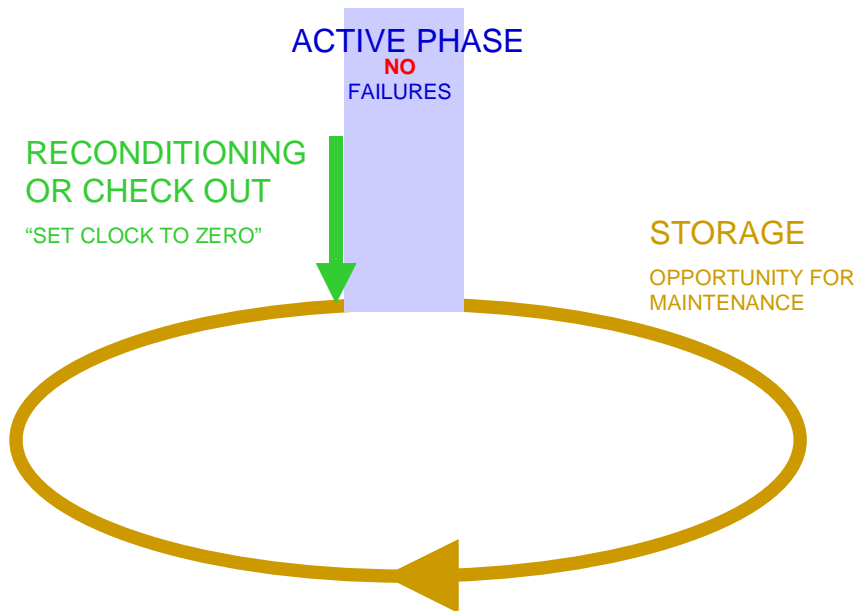


Figure 5: Logistics Cycle of Voting System: Strategy 1

Strategy 2: This strategy focuses on critical failures. Only they are excluded during the active phase. Non-critical failures are permitted and corrected through maintenance actions. The acceptable rate of non-critical failures is mostly determined through economic considerations, but may also be limited in absolute terms. The program that defines maintenance, as well as the logistics system that supports it, is certified as part of the reliability requirement. Careful analysis is necessary to make sure that maintenance work does not breach the integrity of the voting system, and itself cause “critical” failures. It is therefore possible that, at the voting machine level, maintenance is limited to replacement of failed machines.

Figure 6 graphically summarizes the most important elements of Strategy 2.

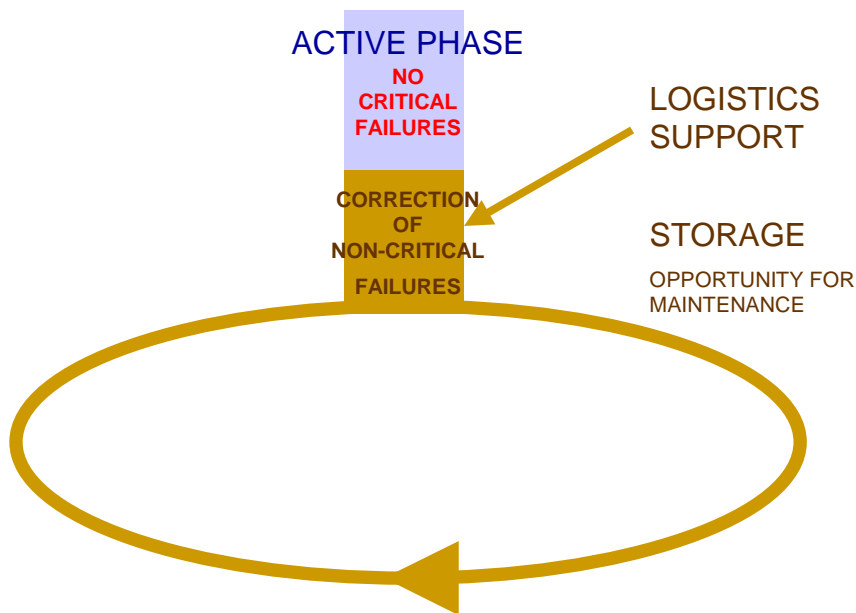


Figure 6: Logistics Cycle of Voting System: Strategy 2

Each one of these strategies has its merits. Strategy 1 is easy to manage, requires no maintenance and logistics organization, at least for the active phase, and works well for simple systems. If properly designed, voting machines could very well be considered simple systems, and subjected to this strategy. One might expect that voting machines under this strategy would be more expensive than those under Strategy 2. However, increasing integration of electronics components may all but erase this difference.

Strategy 2 requires that a management, maintenance and logistics organization be in place during the active phase, including an adequate pool of spare machines. Also, development of a maintenance program that includes anything but machine replacement requires a sophisticated and expensive analysis.

Certification. The two strategies require different approaches to certifying that they meet reliability requirements.

Under strategy 1 it may be possible to simplify the certification criterion to a requirement that the voting machine, under conditions similar to actual operations, will not fail with a frequency that exceeds the prescribed limit. However, analysis of failure mechanisms would be required to exclude “hidden failures,” i.e., failures that themselves do not affect availability of system functions, but may create an opening for other failures that do. This analysis would be performed by the vendor, and audited by the certifying agency.

