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

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

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.

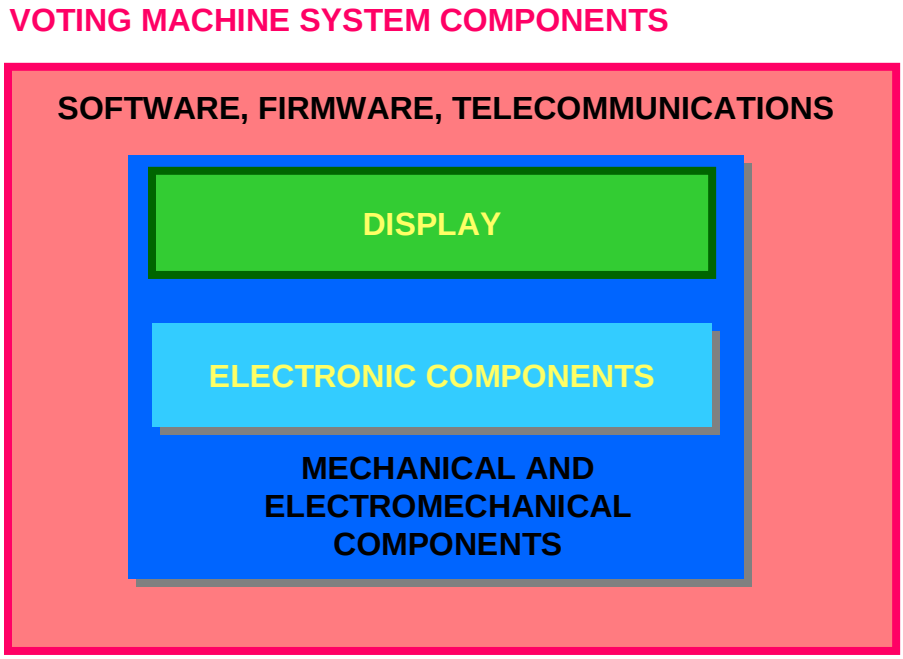

Figure 1

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.

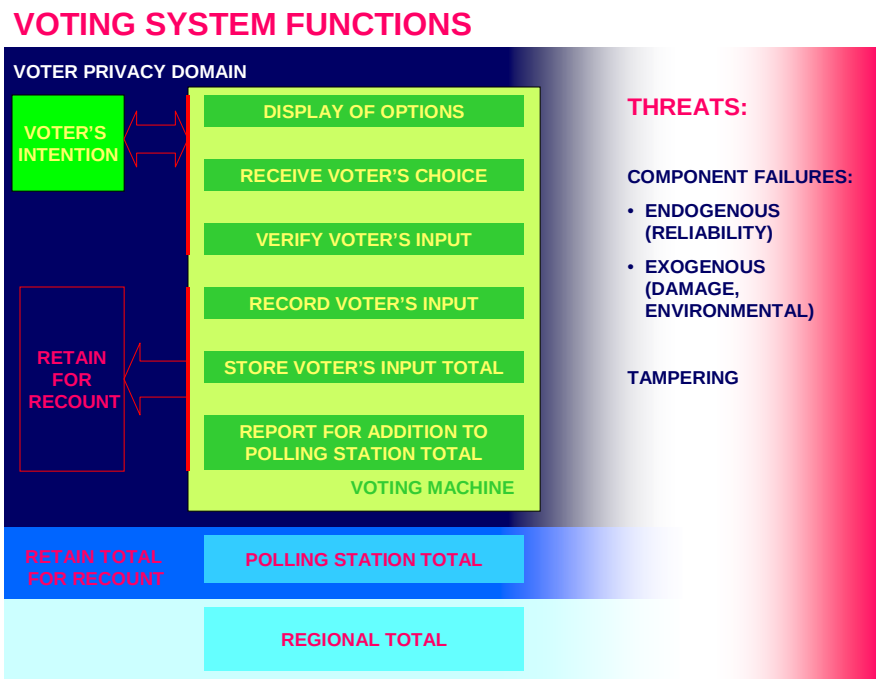

Figure 2

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.

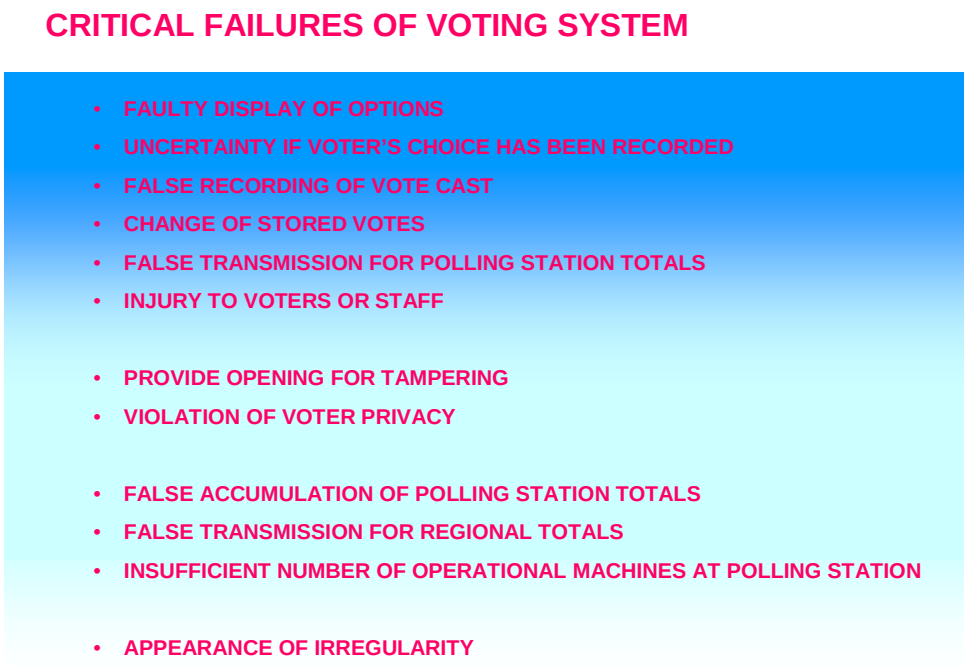

Figure 3

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'etre 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.

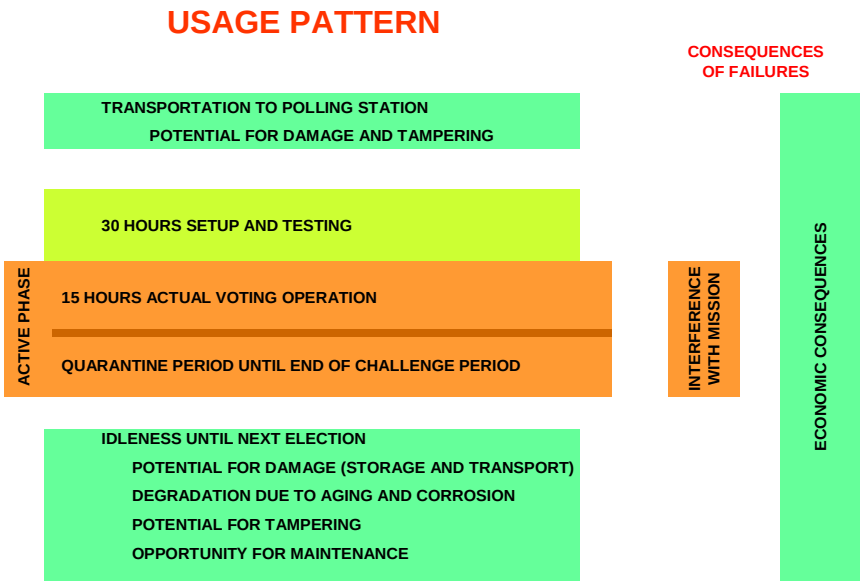

Figure 4

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 be 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.

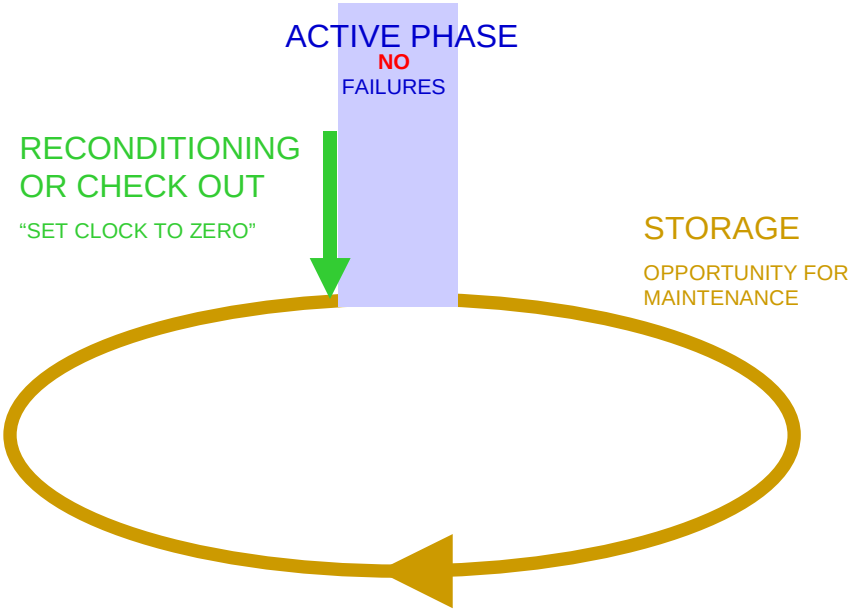

Figure 5: Logistics Cycle of Voting System: Strategy 1

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 though 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.

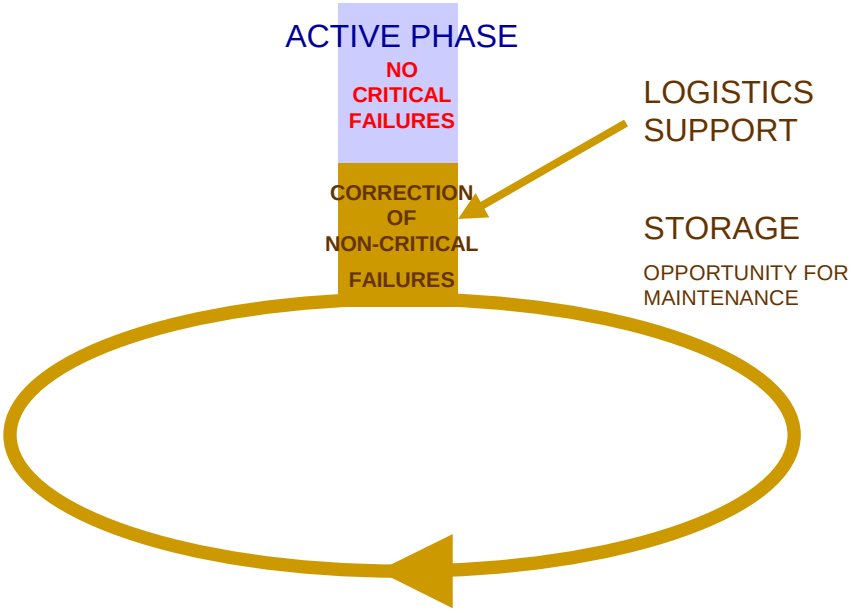

Figure 6: Logistics Cycle of Voting System: Strategy 2

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.

Strategy 2 requires that a disciplined process for managing the logistics system is included in certification of reliability. A prerequisite for this to work reliably is the existence of laws and regulations that impose severe enough sanctions on any violation of the rules.

Like Strategy 1, this strategy requires analysis of functions and failure mechanisms. But this analysis would also examine if the system architecture is suitable to assure availability of all critical functions even as components fail. As under strategy 1, the analysis would be performed by the vendor, and audited by the certifying agency. Also, a jurisdiction would want to see an analysis determining that the system architecture and component reliability support the claims of life cycle cost made by the vendor ("maintainability").

While any jurisdiction procuring and operating voting systems may have a preference for one strategy over the other, there is no need to limit their choice through national guidelines. The Guidelines might therefore best include requirements for both strategies, with the acquiring jurisdiction or state legislature free to select between the two.

Realistic limits on the failure probability.

A benchmark for a limit on the probability of a system failure might be derived from common electronic components of similar complexity. It appears reasonable that voting machines should be expected to not fail at a rate higher than those do. Ronald E. Crane suggests a comparison with *"typical panel computers, including motherboard, CPU, memory, LCD and touchscreen (such as might constitute a DRE's core*) [that] *have MTBFs of approximately 80,000 hours* [VVSG Comments of Ronald E. Crane, 9/21/2005]. Assuming a Poisson failure process, for voting machines this corresponds to a probability of a failure during the active phase of 1.87×10^{-4}.

It should be noted that this number covers critical as well as non-critical failures. It would therefore apply directly to Strategy 1.

Guidance for limiting critical failures in Strategy 2 might be obtained from two sources, Section 4.1.1, Accuracy Requirements, of VVSG2005, and the regulatory practice of the Federal Aviation Administration (FAA).

Civil aviation has long dealt with a mandate to exclude the possibility of critical failures altogether. This is mostly accomplished through design and operating practices. When these practices cannot totally eliminate the possibility of a critical component failure, then the requirement is to keep the probability below 10^{-9}. The probability of a critical system failure is the compounding of all critical component failures, and would thus be significantly larger, although, due to the complexity of aircraft, no hard numbers are available.

For voting machines numbers somewhat larger than those for civil aircraft might be acceptable. Section 4.1.1 of VVSG2005 promulgates a target error rate for each one of a number of processing functions of a voting machine individually of one in 10,000,000

(i.e., a probability of 10^{-7}). (Interestingly, testing is only required to demonstrate an actual rate of at most one in 500,000. It is not clear if this rate is not meant to apply to the compound rate).

An overall systems probability of critical failures in these orders of magnitude would be in line with the benchmark developed, above, for all failures.

The limit on the probability of non-critical failures under Strategy 2 can be set reasonably high. However, if the design of a voting machine is similar to common electronic equipment, then there is no reason to set it significantly below what is already achieved by common electronic equipment. In this case, the difference between Strategy 1 and Strategy 2 might all but disappear.

The MTBF of 163 hours promulgated in VVSG2005 does not represent a failure probability that can be considered "small." Assuming the same Poisson failure process as above, it corresponds to the failure probability of 9.3% determined by [Stanley A. Klein, Statement to EAC on Draft VVSG, September 24, 2005].

Reliability requirements for district and higher level voting systems. At least with current technology, it does not appear reasonable to expect that these systems be designed as "black boxes." Therefore, a strategy like Strategy 2 appears to be the only option.

6. Conclusion

This analysis started out with an open-ended search for a model that would provide a suitable basis for regulating voting machine reliability. An examination of the nature of voting machines, current laws and regulations, and practices in other industries has led to two models that differ only in the assumptions about principles that guided the design of voting systems. Regulation for both strategies can easily stand side-by-side in the guidelines.

Regulation crafted on the basis of either or both of these strategies will differ significantly from what is included in section 4.3.3, Reliability, of VVSG2005.

We have shown that regulation of reliability touches on all aspects of system design and operations. It is interdependent with many provisions that are spelled out throughout the guidelines. Regulation of reliability does not define those other provisions, but it needs to analyze and interpret them in order to develop regulation that best meets the needs and opportunities of the system. As any analysis, this process may uncover potential for a coordinated approach across the entire range of the guidelines. There are semantic issues that may require coordination, as well as definition of functional requirements, and operational processes.

This paper is an effort to set the stage for the future work toward defining reliability requirements. As the next stage, we will examine more closely the experience with

current practice, and collect information on industry structure and cost factors. Based on that, we will formulate processes and metrics that can form the basis for successful new regulation. At this stage, it appears desirable therefore, to start a discussion of all the issues where reliability requirements touch on requirements of other areas regulated through the guidelines.

7. References

The Brennan Center Task Force on Voting System Security, The Machinery Of Democracy: Protecting Elections In An Electronic World, Brennan Center, 2006

Blanchard, Benjamin S., and Wolter J. Fabrycky, Systems Engineering and Analysis, Prentice Hall, 1981

Crane, Ronald E. J.D., B.S.C.S., Public Comments, September 21, 2005, www.eac.gov

Etschmaier, Maximilian M., Mission Oriented Maintenance for Military Aircraft and Implications for Public Transportation Fleet Maintenance, Transportation Research Record, number 958, 1984

Help America Vote Act, www.eac.gov

Klein, Stanley A., Statement to EAC on Draft VVSG, September 24, 2005, www.eac.gov

MIL-HDBK-338B, Military Handbook: Electronic Reliability Design Handbook, October 1, 1998

Nowlan, F. Stanley, Preventive Maintenance, Past, Present, Future, American Institute of Aeronautics and Astronautics, Paper 78-1529, 1978

United States Election Assistance Commission, 2005 Voluntary Voting System Guidelines. www.eac.gov, 2005

VOTING MACHINES: RELIABILITY REQUIREMENTS, METRICS, AND CERTIFICATION

Part 2

Definition of Requirements, Metrics, and the Certification Process

Maximilian M. Etschmaier
September 2006

1. Introduction

In the prequel to this paper [Etschmaier, Voting Machines: Critical Issues for Formulating Reliability Requirements, August 2006], we laid the groundwork for the development of improved reliability requirements for voting machines, and defined how they fit into the overall framework of voting machine design, operation, certification, and procurement.

- We used the term “voting system” to identify the context into which a voting machine is embedded.
- We identified the functions that are required of a voting machine, and differentiated between critical functions and noncritical ones.
- We analyzed the operating environment, including operational (usage) patterns, the maintenance process, and the logistics support system for the voting systems.

The paper showed that there is an opportunity to more closely tailor reliability requirements to the special, intermittent operational pattern of voting machines. Measures other than the currently used mean time between failure (MTBF) were suggested that could be more easily complied with, and lead to better performing voting machines.

The present paper builds on this and charts the course all the way to the process of certifying actual voting machines.

The paper defines a generic voting machine and performs a complete analysis of functional failures for it. Based on the work in the preceding paper, the generic voting machine is divided into a set of components that are identified as the main loci of the major functions required of the machine. An exhaustive analysis of each function, the consequences of losing it, and the failure modes through which it can be lost leads to a definition of reliability requirements for all components.

The analysis also identifies design features that need to be present in order to make it possible to meet the reliability requirements as well as prerequisites that need to be met for any reliability statement to be meaningful.

From the results of the functional reliability analysis, we define a comprehensive metric that can measure the relevant reliability characteristics of a voting machine and that makes it possible to decide whether or not those requirements are met. The metric uses the same model that, applied to the generic voting machine, yielded it. Taking into account the inherent limits of our understanding of systems and technology, as well as the inability of the human to perform logical analyses with absolute certainty, the metric continues to be applied throughout the service life of a voting machine design. During that time, it will be used to verify that the reliability actually is as anticipated. For any deviations, it will trigger corrective measures.

Finally, we outline the process of certification itself.

This paper, just as the prequel, is primarily a contribution to the discussion that needs to occur within the CRT ("Core Requirements Team") group and the TGDC ("Technical Guidelines Development Committee") before requirements can be finalized. Since the requirements identified from the perspective of reliability cut across the whole range of topics that will be covered by the new VVSG ("Voluntary Voting Systems Guidelines"), it is not possible to finalize them solely from the point of reliability. The final form will evolve from discussion and negotiation between all affected areas. Most requirements have therefore purposely been stated in general terms.

An intensive discussion is required so that, over the next months, a final text of the reliability requirements can evolve that is in a form suitable for inclusion into the new VVSG, and that dovetails with the requirements spelled out in the other sections of the VVSG.

2. Functional Failure Analysis of a Generic Voting Machine

Any purposeful system may experience what is commonly referred to as failures. We have defined the term failure as the loss of a system function that results from the malfunction of a part or component. The malfunction may be caused endogenously, i.e., by a mechanism that resides within the component or part, or exogenously, as e.g., by physical damage, by environmental factors, or by tampering.

Depending on the importance of the function, the failure may be "critical" or it may be "noncritical." Critical failures are the loss of a function that is essential to the operation of the system. Proper design will eliminate the possibility of critical failures by assuring that malfunctions are contained before a critical function is lost. If this is not possible or practical, design, operational, and maintenance measures will assure that a failure can only occur with an extremely low probability.

There are basically two ways in which failures can be analyzed:

- One can follow the physical process, or
- One can follow the function.

The first is the path taken by the well-established method of failure modes and effects analysis (FMEA), which is sometimes expanded to include consideration of the level of criticality of a failure. FMEA requires following each physical failure to the point where it runs its course, either causing the loss of a function, or just stopping without any harm. The decision trees that have to be searched in this process can become very large, making the analysis unwieldy and expensive.

The alternative is a functional failure analysis, which is essentially a failure modes and effects analysis process done backward. Instead of focusing on the modes in which parts and components may fail and then determining the functions that would be impacted, it starts by looking at functions and their importance, and examines what physical failures could jeopardize them. The advantage is that a much smaller tree of possibilities needs to be searched, and failure modes can be examined at a much greater level of aggregation.

To make the functional failure analysis efficient, effective, and meaningful, it is essential that the functions are defined well. The functions should be related to the purpose of the system, and they should neither be too narrow nor too wide in their definition. And they should be delineated easily against other functions. To help in the definition of functions, as well as in the analysis, the system is generally first divided into a set of components. Again, no firm rules can be given for this division, except that the components should be separated from each other as much as possible, and they should be of a size that lends itself to an analysis that is neither trivial nor too complex. Clearly, the entire system could be viewed as one component. On the other hand, every part could be regarded as a component.

If the division into components is well-chosen and the functions are well-defined, a functional failure analysis can be very efficient. It is not a mechanical process, however, but does require mature judgment and experience.

A form of functional failure analysis is a standard requirement for determining if the design of an aircraft makes it suitable for the purpose, and, if necessary, for identifying design modifications that will make it so. It is part of the process that is known as RCM ("Reliability Centered Maintenance") or MSG ("Maintenance Steering Group") that is used to define the maintenance programs of airliners. It has been very successful there. However, transporting it to other industries has led to mixed results, most likely because the underlying concepts were not properly translated.

Functional failure analysis is generally applied to an existing system. It will lead to the definition of operational and maintenance procedures and, possibly, to the modification of the design. This is the case in RCM. Contrary to common perception, it is not necessary to possess any operational experience with the equipment that is being analyzed. In fact, the RCM analysis, which goes well beyond a reliability analysis, is performed before any aircraft of the type being analyzed has ever taken to the sky. It is based on the finished design of the aircraft and its components, as well as reliability data obtained from engineering calculations and testing, and engineering judgment.

In the present analysis, the situation is different. There is no finished design, only a generic model. And the purpose is not to develop operational procedures and maintenance programs, but to develop criteria that have to be met by any actual design. Instead of leading to a statement of probability with which failures are expected to occur (or the confirmation that certain failures cannot occur), the present analysis is targeted at identifying design features that will assure that failures cannot occur or will only occur with a very small probability. Only a small adaptation is necessary to accomplish this.

For the purpose of analyzing a generic model, functional failure analysis is the only option since, per definition, the detailed design required for a failure modes and effects analysis is not available. The functional failure analysis is easily adapted to defining reliability requirements. The procedure we have used is based on an adaptation of concepts that we have incorporated in frameworks of Mission Oriented Maintenance and Dynamic Maintenance that we have applied to a wide variety of systems.

2.1. Functional Model of a Generic Voting Machine

A functional model provides a structure for a system (voting machine) by breaking it down into more manageable elements (components) and defining a role for each element as well as rules by which the elements interact with each other. There are usually different ways in which the structure of a system can be defined. For any purposeful system, the choice of structure is affected by the purpose of the system as well as the environment.

There are no hard rules for how to divide a system into components and functions. We have used the definition of functions in the preceding paper [Etschmaier, Voting Machines: Critical Issues for Formulating Reliability Requirements, August 2006] as a guide to define components that are logically and physically as distinct as can be expected. This definition makes it easy to state reliability requirements as well as to identify necessary design features.

Following is the list of the generic components.

- A module ("Options Generation") that generates the ballot styles to be used for an election cycle and enters them in the memory of the voting machine before the start of the election. This module need not be part of the physical voting machine. One module can set up the data structure for many voting machines, and many different ballot styles. The communication from this module penetrates the main part of the voting machine. Precautions, therefore, are necessary that this communication is used only for the intended purpose.
- A module ("I/O control program") that controls the voting I/O process for a voter. It defines the ballot that is presented to the voter, manages the interaction with the voter, and delivers a valid ballot to the repository. The program of this module is part of the voting machine design, certified as part of it, and loaded into the machine upon manufacture. It should not change over the life of the voting machine.
- An I/O data module that stores the ballot styles and validation rules for ballots that are entered by the options generation module.
- An I/O device through which the voter interacts with the voting machine. This module generates the ballot based on the data provided by the I/O control program, and displays it for the voter. It receives input from the voter, serves as I/O device for the vote validation process, and transmits the vote to the I/O control program. It should contain its own drivers so that the communication with the I/O control program can be limited to data. This unit could be a standard commercial item that is verified so that it does not contain any distracting code.
- A core control program that manages the repository of votes. This module receives data from the I/O control program, deposits them into the repository of the core data module, and retrieves them from there for transmission to the precinct-level system.
- A core data module that stores all votes cast on the machine with the required level of detail. The data stored in this module need to be held until all possibilities of a recount have been exhausted or as long as required by law. Depending on the design of the voting system, instead of holding the data inside the voting machine, they might be transferred to an external storage device after the election.
- The "machine core" which is made up by the physical structure, conduits, and connectors that holds all other components together and provide a physical barrier against threats to the integrity of the voting machine from the outside.

- An alternate path for recording the results of the voting. Such a path may or may not be required by the laws and regulations governing the election. Generically it will be identical to the main path defined here.
- A verification unit through which the proper functioning of the voting machine, including the ballot styles and associated rules stored in it, can be verified before, during, and after the election. This unit is not part of a voting machine, but rather serves many voting machines. It communicates with the voting machine only through data.

Figure 1 shows these components, and how they are connected.

We expect that an actual design of a voting machine that follows this delineation of modules will not only make an analysis easy, but will also lead to a system with a high reliability rate. It would also greatly expedite the certification process. However, there may well be other definitions that might appear more suitable to some vendor. The guidelines might, therefore, leave it up to a vendor to choose which partition to use in their systems and in the analysis they provide to the certifying agency.

The figure also shows boxes around groups of components to indicate how they are linked logically, physically, or in the certification process. The color-coding of these boxes is shown in the figure. Dashed lines indicate optional elements or links; e.g., the operations generation module may be physically attached to the I/O module, or it may be implemented as a separate unit that can provide input to a number of voting machines. Also, keeping an alternate record, in whatever form, might or might not be required. The corresponding path and component, therefore, are shown as optional.

With each component, we also show the interactions it has with other components. The box colored in light green and framed with a solid green line represents all the physical elements that tie the voting machine together. We refer to them as machine core. They include the physical structure and enclosure, the power supply, the devices that contain the I/O channels, and any other ancillary components that might be provided.

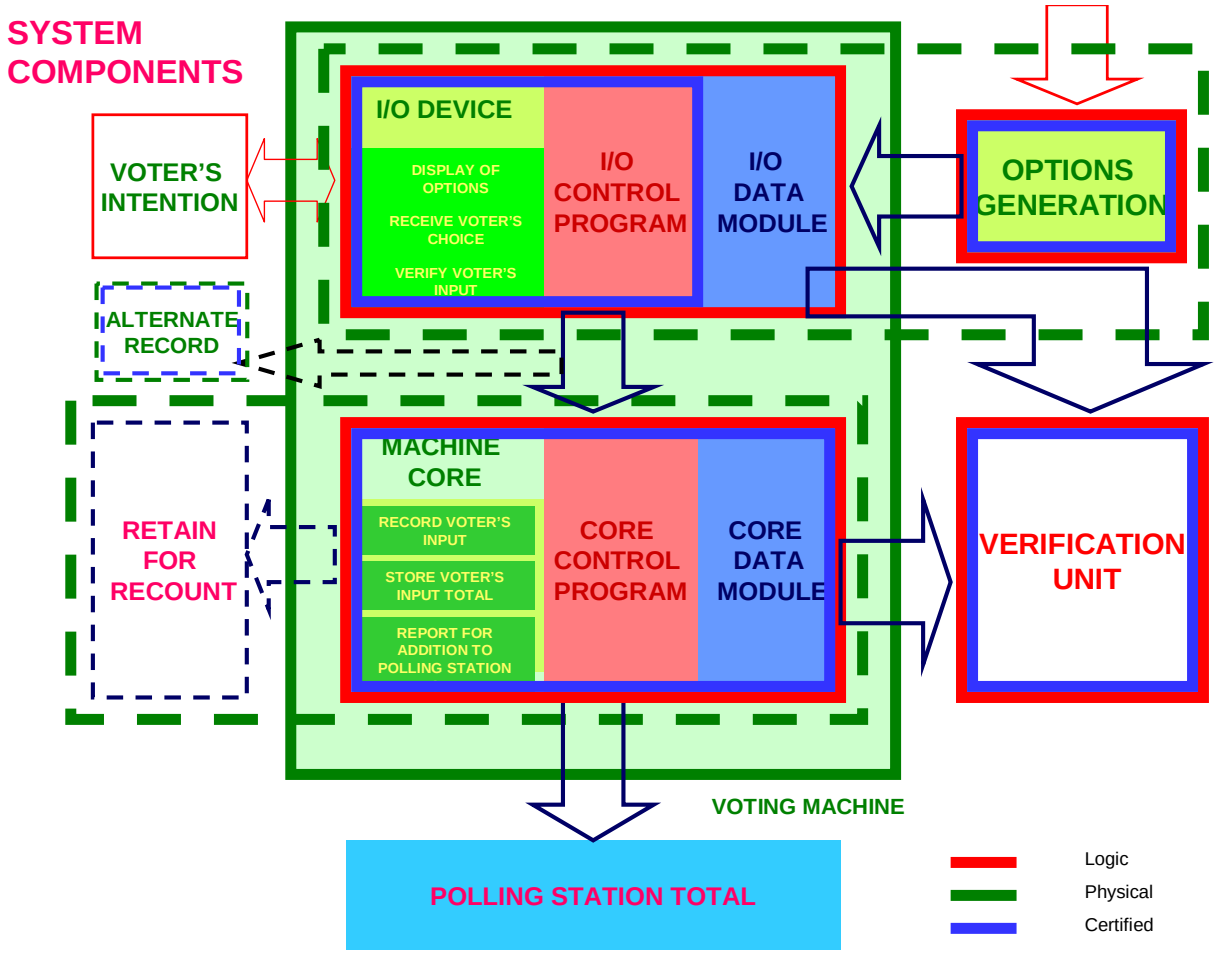

Figure 1

Generic system components of a voting machine

2.2. Summary of Results of the Functional Failure Analysis

The functional failure analysis examines every component, identifying the functions that are required of it, the level of criticality of each function, and the ways ("modes") in which it can be lost ("functional failures"). Finally, it finds means by which critical functions can be protected, i.e., be kept from failing or kept to an extremely low failure rate. It also assures that probabilities of noncritical failures are kept within defined limits.

Much of the protection can be provided by the system design. Certification will ascertain that the features that are required to achieve the required protection against failures will indeed be available and work as required. Only the failures that cannot be eliminated through design measures require specification of a reliability target.

Design requirements are a prerequisite for meaningful reliability requirements. The requirements that were identified in this analysis follow in many ways the example of the Technical Standards for Gaming Devices and On-Line Slot Machines of the State of Nevada. However, what is included here as design requirements is only what appears necessary from the point of view of defining reliability requirements. Development of a comprehensive set of design requirements and framing them in a format that is suitable for inclusion in the VVSG document is not part of this paper and will be addressed by others.

In the following discussion, the reliability requirements are summarized by generic component. Included in the summaries are requirements of component functionality that need to exist for the reliability statement to be meaningful.

The reliability requirements are identified in general terms as those for critical failures and those for noncritical ones.

Many parts that go into these components will be standard commercial products. Irrespective of the component requirements, it appears reasonable to expect that these parts comply with the same reliability standards that parts used in similar systems under similar circumstances are expected to meet. For parts that can cause critical failures, only the highest reasonably achievable reliability rate seems acceptable. Since this rate keeps improving over time, it might be reasonable, instead of specifying a hard number, to define the standard in general terms. The certifying agency might publish, and from time to time update, a concrete number for every type of part. The number that is in force at the time of certification of a voting machine would be the one that applies.

There are existing regulations that specify targets similar to what is suggested; e.g., the Clean Air Act Amendment of 1990 requires certain pollution control equipment and processes to be based on "Reasonably Available Control Technology**"** ("RACT"), and in some cases, on "Maximally Available Control Technology**"** ("MACT").

2.2.1. Component summary for the voter I/O device

The I/O device is the key interface of the voting machine to the voter.
The possibilities for this system component to cause critical system failures are

- That it fails to operate, leaving uncertainty about what data have been transmitted, and
- That it transmits code to the control unit.

Proper system design will eliminate the possibility of this failure or limit its frequency to that for critical component failures.

The possibility of a noncritical failure is that it ceases to operate, shutting down the entire voting machine, but not causing uncertainty about accounting for votes cast.

Design attributes that require certification are:

The I/O device is a self-contained unit that operates separately from the control unit. It contains all the software and hardware elements necessary for its operation, and transmits to other system components only data.

Certification will attest that the component:

- Is free of software errors,
- Contains no code elements that can cause it to send code to the control unit, and
- Meets the reliability requirements specified below.

Reliability requirements:

- If the possibility of a failure leading to uncertainty whether a vote has been recorded cannot be excluded: Limit the probability of failures to that for critical failures.
- Otherwise: Require the component to meet the failure probability for noncritical failures.

2.2.2. Component summary for the voter I/O control program

The control program manages the I/O process. It presents data to the I/O module, receives data from the I/O module, and validates input. It transmits the vote to the recording module when commanded by the voter. It also provides information to the verification unit when queried. It is required to transmit nothing else.

Failures of this unit can be critical. Data can be corrupted, and upon a hardware or software failure, there can be uncertainty if the voter input has been recorded.

It may be possible to eliminate this possibility for software failures by proper design of the software. However, it may be difficult to exclude this possibility for failures of any of the hardware components, especially processor and I/O channel. The reliability criteria for critical failures therefore apply to the entire hardware.

Design attributes that require certification:

The control program, together with the I/O channels, should be designed as a self-contained unit that does not interact with the environment, except through data. The functionality of this unit is mostly determined by software, although malfunctioning hardware elements can interfere with (damage) loaded software and stored data. It does not appear that hardware failures can be eliminated entirely; however, since they can be or cause critical failures, they have to be limited to the probability allowable for those. Prerequisites for program certification are that the software is transparent, is functionally verifiable, and does not contain code that is not used. It must not be possible to modify the software after certification from outside, or that the software modifies itself. A nonvolatile, non-erasable medium appears to be a prerequisite.

Reliability requirements:

Software failures should be eliminated through design measures. Since all hardware failures can be critical, they have to be limited to the rate allowed for critical failures.

2.2.3. Component summary for the I/O data module

This data module is a storage device that contains the ballot data for an election, including the rules to determine correctness of a ballot. It does not contain votes. A failure (hardware) might go unnoticed, but might alter the data in a way that would change how the ballot is presented to the voter, or validated. Unless the possibility of an alteration of data can be excluded, the component is a critical component**.**

Design attributes that require certification:

This module can be based on a standard product that provides nonvolatile, write once-read many storage. Provisions need to be made that the module cannot be written to after initialization. Certification is required for the hardware attributes, as well as for the procedure that writes data to this module. Certification will attest that the component hardware meets the functional requirements, and has a failure probability that meets the standard for critical failures.

Reliability requirements:

The failure probability meets the standard for critical failures.

2.2.4. Component summary for the machine core module

This component provides the physical infrastructure into which the other modules of the voting machine proper are embedded. It includes structural elements, possibly a cooling mechanism, the power system, and the communications conduits. If all the software is designed so that physical failures are contained and cannot lead to critical consequences, then, by definition, a failure of this unit cannot be critical. Even if there is only a chance of that condition not being met completely, though, reliability requirements for critical components should be applied.

Design attributes that require certification:

The physical structure, the power supply, and the communication conduits need to be suitable for the purpose. Certification will attest that the component is suitable, and meets reliability requirements defined below.

Reliability requirements:

If the criticality of software failures cannot be ruled out, the standard for critical failures applies. Otherwise the standard for noncritical failures is adequate.

2.2.5. Component summary for the options generation module

The options generation module may not directly be part of the voting machine but might be attached to it only for the purpose of initializing the data module with data it generates from information entered into it. It is used only before the election cycle. If the data module is removable from the voting machine, the options generation module may never touch the voting machine. One unit may initialize many voting machines, and with different data. However, an undetected fault in this module can cause incorrect data to be loaded into the data module that might not be detected even by the verification module. Malfunction of this module is critical only if it alters the data that are entered into the voting machine from it and if these alterations are not detected. However, this standard may not be achievable. As a practical matter, it might be desirable to make the hardware reliability standard compatible with the strict performance criteria for the software.

Design attributes that require certification:

Certification will verify the functionality of the software that transforms the input into the data that are generating the ballot and the rules of voting inside the voting machine. Certification needs to determine if hardware failures can affect the information transformation, and if, therefore, reliability standards for critical failures have to be met. Certification will attest that this unit correctly validates data, correctly formats data, sends correct data, and will not send code through output channel. If hardware failures can lead to critical failures, the hardware reliability requires certification to the standard for

critical failures. Prerequisites for program certification are that the program is transparent, is functionally verifiable, and does not contain code that is not used. The design must be such that, after certification, the program cannot be modified from outside, or cannot modify itself. Any software error rate must be limited to the level permitted for critical failures.

Reliability requirements:

If hardware failures can cause critical failures then the hardware reliability has to meet the standard for critical failures. Otherwise, failures will only affect the election preparation where in many cases there would appear to be enough slack to compensate for failed units. However, to avoid bottlenecks, and limit the requirement for spare units, it appears desirable to require the reliability of this unit to at least meet the standard for noncritical components.

2.2.6. Component summary for the core control program module

The control program module receives data from the I/O control program, stores it in the data module, and, upon request, passes information on to the precinct-level system and to the verification unit. The function of this component is clearly critical. However, if it is designed in such a way that hardware failures cannot affect the integrity of data or alter programs in a way that may not be detected immediately, then failures might not be critical. Since this is unlikely to be possible, reliability requirements for critical failures ought to be applied.

Design attributes that require certification:

Certification will attest the proper functioning of the component as well as the reliability. Prerequisites for program certification are that the program is transparent, is functionally verifiable, and does not contain code that is not used; and that after certification, the program cannot be modified from outside nor modify itself. If software errors cannot be excluded, their impact needs to be limited to the standard for critical failures.

Certification needs to attest that this module properly receives data, correctly enters it into storage, and correctly retrieves it and passes it on to the precinct level system and to the verification unit. Certification will also examine if the module provides proper protection against physical failures causing critical consequences. If standard hardware components are used, it would appear sensible that they be required to be certified by an established authority to standards of functionality and reliability compatible with these requirements.

Reliability requirements:

Since it is unlikely that the design of this module can provide total protection against physical failures leading to critical consequences, reliability standards for critical components apply. Otherwise, reliability standards for noncritical failures would suffice.

2.2.7. Component summary for the core data module

This module accumulates votes. It stores the votes so they can be retrieved for transmission to the precinct-level system, and for a possible recount. It only interacts through the control program. A failure of this component can corrupt the vote count. The failure consequences are limited if a nonvolatile device is used that can only be written to once and that cannot be overwritten or erased. The device will contain a mark that identifies the end of data for one election. This is a critical component.

Design attributes that require certification:

Certification will attest the proper functioning of the component as well as the reliability. A prerequisite for certification is that the data storage is transparent and verifiable, and that it can hold a mark that unambiguously identifies the end of data for one election, and that cannot be altered. It is to be expected that a standard hardware component is used, and certification by an established authority would be available. Additional certification could be limited to assuring that the outside certification standard meets the functions requirements spelled out above, as well as the reliability requirements for critical components.

Reliability requirements:

The reliability requirements are those for critical components.

2.2.8. Component summary for the verification unit

The purpose of the verification unit is to ascertain conclusively and unambiguously that the voting machine is properly configured for a specific election. One verification unit can verify many voting machines. Reconfiguration for different ballots ought to be possible. Verification should be possible before, during and after an election. The unit will obtain information from the voting machine and will not send information, neither data nor code, to it. The only exception is the data that may be required to initiate the verification process. The verification unit will perform an exhaustive verification that will detect any discrepancy in data or functionality. The verification program will be based on the certified design of the voting machine. If the verification misses a critical discrepancy in the voting machine, this will constitute a critical failure. The requirements for functionality and reliability for this unit are, therefore, those for critical units.

Design attributes that require certification:

Both the hardware and the functionality of the software require certification. It should be expected that most hardware components would be standard commercial items. They should be expected to be certified by an established agency to a standard that meets or exceed that for critical components. A prerequisite for program certification is that the program is transparent, is functionally verifiable, and does not contain code that is not used; and that after certification, the program cannot be modified from outside, nor modify itself. If software errors cannot be excluded, their rate needs to be limited to the standard for critical failures. Certification will attest that the component correctly verifies a voting machine, will not send data or code, will not accept code through I/O channels, and will not receive data through output channels.

Reliability requirements:

Unless the possibility can be excluded that hardware failures will lead to critical failures, reliability requirements for critical components apply. In fact, since one verification unit may verify many voting machines, the consequences of a critical failure might be significantly more severe than it is there. A higher reliability standard would therefore be justified. For comparison: the standards for gaming machines in Nevada require error rates in verification units to be less than 10^{-38}.

2.2.9. Component summary for the alternate record

Many different arrangements are possible for storing votes in an alternative record. The purpose of prescribing an alternative way of storing the votes is to increase the confidence in the election results. However, if there is any difference between the totals from the two records, unless there is an unambiguous method for resolving the difference, the effect might be the opposite. Any difference in the totals for the two paths is a critical failure.

Whatever method is chosen for creating an alternative method, therefore, will need to satisfy the following criteria:

- It needs to start out with an input that is identical to that entering the main path.
- Together with the main path, it needs to meet the requirements for critical failures.
- The resulting reliability requirement for either path is therefore higher than the reliability requirement if only one path were used.

Design attributes that require certification:

The alternate path will have components and attributes that are equivalent to those of the main path. The same requirements apply. The certification is equivalent to that for the main path.

Reliability requirements:

The reliability requirements are the same as those for the main path. The requirements for each derive from the requirement for the two together. The highest overall reliability is achieved if both have the same reliability.

2.3. Summary of the System-Level Requirements

Functional failure analysis develops a model of the voting machine. The model identifies the failures that may occur, determines the degree of their severity, and the frequency of their occurrence. By imposing limits on the failure severity and rates, it is possible to identify those design features that cause the limits to be exceeded. The model permits the design features to be varied until all imposed limits are met.

By applying functional failure analysis to a generic voting machine, instead of an actual design, it was possible to use the analysis to identify requirements that have to be met by any design to satisfy the defined limits.

The limits that were applied are:

- Failures that cause the loss of a critical function ("critical failures") must not be permitted to occur. If their occurrence cannot be avoided, they have to be limited to a very low probability of occurrence. A concrete numerical value will be attached to this limit in a later analysis.
- Other failures must be limited to probabilities that are defined by economic and other considerations. A future paper will provide guidelines for the necessary analysis.

The component requirements span the entire voting machine. There are no failures that can happen outside the components. However, any failure of a component is viewed as a failure of the voting machine by the higher-level system into which the voting machine is embedded. Concretely, this is the precinct-level system.

As described in part I of this report, not having the minimal number of voting machines available at a precinct is a critical failure of the precinct-level system. Protection against this failure can be achieved if more than the minimally necessary number of machines is assigned to the precinct.

The number of spare machines required to protect against a situation where there is an insufficient number of machines at a precinct is determined by the probability of a failure of any one machine, the number of machines available at the precinct, and the minimal number of machines required to satisfy the demand. It can easily be obtained through standard probability analysis. Conversely, one can determine the level of protection provided by a given number of spare machines and check if that level is sufficient.

In the first report, we introduced two strategies for determining the reliability requirement.

> Strategy 1 assumed that there would be only one group of failures that might include critical as well as noncritical failures. The probability of their occurrence would be kept very small.

Strategy 2 permits noncritical failures to occur at a rate that is determined by economic optimization. Our analysis has shown that under certain conditions, two components may be permitted to incur noncritical failures:

- The I/O device, and
- The physical system core.

If the I/O device is configured and implemented in such a way that it can be removed from the voting machine without a chance of violating the integrity of the machine or the data and programs stored in it, then it is possible to swap a malfunctioning device with a working one during voting. Instead of keeping a spare voting machine to cover a malfunction of the I/O device, it might therefore be possible to store just a spare I/O device. However, it would be necessary to have a qualified person at the polling station that can properly carry out the swap.

While the probability of a failure in these components may be orders of magnitude above that permitted for critical failures, it could still be kept to a value small enough to call for no more than one spare unit per typical polling place.

However, there is already a spare machine at each polling place to cover for critical failures. It is not expected that, if the probability of critical failures is kept the prescribed value, there will be much demand for this unit. It might be possible to use that machine also to cover for the failures of the I/O device. This would obviate the need for a spare I/O device, for a significant cost reduction.

It is not likely that noncritical failures of the physical core can be corrected during the voting process without jeopardizing the integrity of the voting machine. A failure, therefore, needs to be covered by a spare machine.

In summary, it is likely that with properly designed voting machines failure probabilities will be so low that, for a typical precinct, all categories of failures can be covered by one spare voting machine. The usefulness of Strategy 2 would then be eliminated.

The rules for determining the spare machine requirements only affect the one critical failure of the precinct voting system that we have identified. They do not affect the reliability requirement of the voting machine, and therefore should be defined in a separate requirements document.

2.3.1. Prerequisites for Reliability requirements to be meaningful and achievable at election time

The analysis identified a number of conditions that have to be met by the design of the voting machine. These conditions can be grouped into three categories: the functionality of the machine will permit the necessary analysis and prevent malfunctions from leading to critical failures; transparency will permit verification that the functionality meets requirements and conforms to claims by the vendor; and integrity assures that the voting machine that is used in the voting process conforms to the voting machine that has been certified. In the following discussion each one of these conditions will be examined further.

2.3.1.1. Functionality

The voting machine is required to provide the functions that define its operations. These functions were defined in the first report and form the point of departure for the reliability analysis. To permit an efficient analysis, it is required that the voting machine does not include functions that are not needed for the performance of these functions. It should be ruled out that extraneous functions, such as election management or the poll book, are tagged onto the voting machine.

In the course of the analysis, it was discovered that the way the functions of the voting machine are implemented can help stop malfunctions from leading to critical failures. The additional functional requirements that result from this are:

- The software must be free of errors. Should it not be possible to eliminate software errors entirely, the rate of errors must be limited to the level permitted for critical failures.
- The software may not contain code that is not used. This requirement would seem to eliminate the use of general-purpose software. Software may not contain code elements that can cause sending or receiving code to the other components.
- It must not be possible to send code through I/O channels.
- It must not be possible to receive data through output channels or send data through input channels.

2.3.1.2. Transparency

Only transparent functions can be verified directly. Verification of functionality through alternate methods like statistical analysis or simulation is neither necessary nor would it provide the degree of certainty and confidence that should be expected of a system used as critical input to the election process. The following transparency requirements were identified through our functional analysis:

- Functions need to be clearly defined in the system design. They need to be verifiable through an analysis of system design documents and printouts, as well as traceable through operational tests.

- The components used in the voting machine need to have clearly defined functionality, boundaries, and interactions.
- The software must be transparent and functionally verifiable in every detail.
- The data storage must be transparent and verifiable, and capable of holding an unalterable mark that unambiguously identifies the end of data for one election.

2.3.1.3. Integrity

Voting machines are certified at one point in time. Thereafter, copies of the certified machine are produced and introduced into the actual voting process. The certification is only valid if

- There is assurance that any voting machine is a true copy of the certified original.
- Nothing in the voting machine may be altered after certification.
- The voting machine should not be able to alter its own functionality.

Any change to the voting machine that may be considered necessary or desirable for whatever reason will require a new certification. At the option of the certifying agency, not all the analysis and testing required for a full certification may be mandated.

The need for integrity also affects the operation of the voting machine during the voting process. Assurance of proper functionality throughout the voting process requires that the voting machine not be interfered with other than through the voting process performed by the voter. Specifically this requires:

- That no maintenance work whatsoever be performed on the voting machine during the election process.
- That either the security of the voting machine from one voting process to the next can assure the integrity of the voting machine, or the voting machine undergoes a complete functionality check before every election cycle.
- That all data stored in the voting machine are protected from the beginning of the voting cycle (i.e., if applicable, immediately after the functionality check) until the end of the period for recounts.

The functional failure analysis has shown that, therefore,

- Software and data need to be stored in a nonvolatile, non-erasable medium.
- It must not be possible to modify the software from the outside after certification, nor can it be possible that the software modify itself.

3. A Metric for Defining Voting Machine Reliability Requirements

Metrics are system models that express a system attribute or an aspect of system behavior in terms of a concise expression. A well-chosen metric will permit judgment about the level of performance of the system and its suitability for some purpose. Obtaining the expression may involve analysis and/or testing of the system.

The metric for system reliability defined by VVSG2005 is the "mean time between failures" of the system. The concept of failure underlying this definition is specified in general terms, only applied to the "voting system" as a whole, and does not examine the progression of failures through a voting machine. The metric is valid only when the failure process follows a particular model, and unnecessarily constrains equipment design for a process that only goes on for a very short time. Measurement of the metric is limited to physical testing of the voting machine. The requirement for certification is very low. Consequently, this metric has been widely criticized as inadequate.

The present analysis has shown that it is possible to design and build voting machines that meet much higher standards of reliability. Those higher standards will be sufficient to provide a basis for elections that will not be tainted by lingering questions about the validity of the result. They are expressed in the form of a comprehensive metric that is proposed as the basis for specifying the new reliability requirements for voting machines.

The metric that has emerged from our analysis (the "Voting System Reliability Metric") is a statement of the possibility of critical failures and of the probabilities of noncritical failures of the components of a voting machine. Those statements are obtained through applying a specific analysis procedure to a voting machine.

The analysis procedure follows the functional analysis model used in this paper. However, the objective is different. Whereas the analysis in this paper was intended to determine requirements, the analysis of the actual machine will determine if those requirements are met.

The certifying agency will issue specific guidelines for the performance of this analysis. These guidelines may specify a specific format, or they may leave the choice of format up to the vendor, as long as they use a format that allows verification of the analysis. A prescribed format would standardize the analysis, and could simplify and shorten the certification process.

A voting machine will be considered fit for the purpose if the application of the Voting System Reliability Metric yields a statement that satisfies the following requirements:

- There should be no possibility of critical failures occurring. In many cases, it will not be technically possible to accomplish this goal. In those cases the probability will be limited to a very small value. That value will be specified by the certifying agency. It should be in the order of 10^{-9}, the number used in civil aviation.

- Noncritical failures are identified through the analysis process together with critical failures. Instead of assuring that they may not occur at all or at most with a very small probability, these failures will be analyzed with respect to their impact and the potential for controlling their probability of occurrence. Limitations on the probability of their occurrence could be set by economic analysis. However, since they cause an interruption of the voting process, the certifying agency may set a relatively high absolute limit.

For voting machines that cannot meet this standard, application of the Voting System Reliability Metric will yield information on how to improve the design so that they can.

3.1. Limitations of the Voting System Reliability Metric and Resulting Reliability Performance Monitoring Requirement

Use of the Voting System Reliability Metric requires diligence in the performance of the analysis as well as the application of state-of-the-art engineering knowledge. Review of the analysis will provide "a second pair of eyes" to assure that the analysis is correct and complete. However, the state of engineering knowledge is constantly evolving, and no level of diligence can eliminate the possibility of human error. These two observations then define the limitation of the metric, as they define limitations of any other conceivable metric. By recognizing these limitations, the certifying agency can assure that the voting systems certified to the Voting System Reliability Metric will meet the test of time.

Limited engineering knowledge and human error will lead to system performance below what is expected from the Voting System Reliability Metric. Failures will happen that are not supposed to happen. Some failures will lead to critical failures that were supposed to be impossible. This occurs in all technological systems. There is little point in demanding a better analysis since that is intrinsically impossible. Instead, the route to take is to manage the situation through systematic monitoring of actual system reliability performance[1]. The monitoring process takes on the role of a feedback loop in a system that can be viewed as a reliability management system.

Monitoring the actual reliability performance will help identify the existence of instances where the actual reliability deviates from what was anticipated by the analysis model. Discovery of a deviation will trigger a search for the cause. Understanding the cause of a problem, in turn, will lead to development of a correction, most likely in the form of a design modification.

Given the imperfection of our world, a systematic performance monitoring process, together with the corresponding design improvement process, is an essential requirement for assuring voting machine reliability over the lifetime of a voting machine design. Without it, even the "best" design will fail to perform satisfactorily in the long run.

[1] The input for this process comes from the local election officials through appropriate state agencies.

The described limitation of the Voting System Reliability Metric is not to be confused with an acceptance of shoddy analysis. Given what is at stake, and given the relatively large number of voting machines that are needed, there is no reason to tolerate anything but the very best effort in the performance of the analysis.

It is recommended that the new guidelines include specifications for the reliability performance monitoring and design improvement process.

4. Certification and Testing of Voting Machine Reliability

The certification issues addressed in this section are limited to those issues that are necessary to determine that some given voting machine design conforms to the reliability standards defined in this paper. The standard is expressed in the form of the Voting System Reliability Metric that is defined in Section 3. As described in Section 3, the metric is a large analysis model that is applied to a voting machine design. The model requires that certain conditions of functionality, transparency, and integrity be met by the voting machine. A voting machine that does not meet these conditions cannot be certified, either because a statement of reliability would be meaningless, or because the analysis would not be possible.

4.1. Required Content of Submission

A vendor seeking certification of a voting machine will provide to the certifying agency the following:

i. A number of identical specimen voting machines that are identical in all aspects to the machines the applicant is seeking to sell. These machines will be subjected to volume testing[2] by the certifying agency. Most will be returned to the applicant after completion of the test. A small number will be retained by the certifying agency as reference models and for the performance of future testing that the agency might consider desirable.

ii. A detailed and complete documentation of the voting machine, its functions, components, and supporting design analyses and calculations.

iii. A detailed and complete documentation of all software incorporated into the machine, and a complete and detailed report documenting exhaustive testing of the functionality of the software.

iv. A complete functional failure analysis in the format specified by the certifying agency.

v. Certification documents or test results documenting the reliability of parts and components incorporated into the voting machine. Any test results require certification by an authorized testing laboratory.

vi. Reliability analyses and testing used to determine the failure probability of all components of the machine. Any test results require certification by an authorized testing laboratory.

[2] In a volume test a larger number of machines are operated through a number of simulated election cycles.

vii. An enforceable assurance that the applicant is qualified and financially fit to provide technical support for the machine over its projected service life. The support to be provided includes monitoring the in-service performance of the machine, and developing fully justified and certifiable modifications to the machine that are suitable to correct discovered deficiencies.

viii. A sworn statement by an authorized representative that the submission is complete and that there are no facts or circumstances known to the company that might negatively affect the certification of the machine, and have not been revealed by the company.

4.2. Examination and Verifications Performed by the Certifying Agency

The certifying agency or an appointed agent will examine submissions ii through vi for compliance with the following criteria (This list contains only the examinations that are necessary for certification of compliance with the reliability requirement. Many of the examinations will also serve other purposes. Their descriptions may need to be amended to cover what is required for those. Other examinations may need to be added to determine compliance with other requirements.):

i. Completeness of submission and compliance with format requirements.

ii. Verification that the submitted machine provides the functionality required to make it fit for the purpose.

iii. Verification that the submitted machine does not include functionalities that are not needed[3].

iv. Verification of the reliability certifications, calculations, and tests for compliance with the requirements defined in these guidelines and in subsequent implementation directives for parts and components. The certifying agency may require the applicant to provide additional documentation, analysis, or verification, and to conduct additional testing. The agency may also conduct its own tests using the specimen included in the submission or on additional materials requested from the applicant.

v. Verification of the functionality of the software and the testing provided by the applicant. The certifying agency may require the applicant to provide additional documentation, analysis, or verification, and to conduct additional testing. The agency may also conduct its own tests using the specimen included in the submission or on additional materials requested from the applicant.

[3] This does not affect the ability of the vendor to offer the same voting machine type to states with different requirements. Configuring a voting machine for these requirements is done through the options generation module.

vi. Verification of the functional failure analysis and determination that the conclusion of the analysis provided by the applicant is justified.

4.3. The Volume Performance Test

Testing of the voting machines is an ongoing process that starts with the volume test of the certification process, and continues during every election. A program to monitor the in-service performance of the machines will assure that the machines will perform as required over their entire service life. Feedback from this monitoring will lead to modifications of the machines as required to achieve and maintain the required level of performance.

The analysis and component reliability testing are designed to assure that the machines can meet the required performance targets. The volume test included in the certification process is designed as a final check that these analyses are valid and correctly forecast the behavior of the machine under the realistic condition of the voting day. They will provide the ultimate level of confidence about the machine to the election officers and the general public. They may also serve to validate operating instructions, human factors issues, and serve as vehicle for user training.

The test will put M machines through N election cycles. No more than one failure will be acceptable for the entire test. Concrete values for M and N will be determined such that the occurrence of one or fewer failures during the test can be confidently interpreted as being the result of a sufficiently small failure probability.

Consistent with the real voting operation, there will be no maintenance, modification, or other violation of the integrity of any voting machine during the test cycle.

Monitoring the in-service performance of the voting machines will serve as the indefinite extension of the volume test. The monitoring program includes collection of data of in-service failures and difficulties, continuous evaluation of these data, and corrective actions if the observed failure rate suggests the conclusion that the failure probability exceeds the acceptable limit.

Collection of data is the responsibility of the jurisdiction operating the voting machine. The manufacturer will maintain a technical staff that will monitor the in-service performance, evaluate discrepancies, and develop and carry out corrective actions. The certifying agency will supervise this process, and if necessary, order corrective measures. The orders may include that voting machines not be used in elections until identified problems are corrected.

Monitoring the in-service performance is required to keep the certification of a voting machine in force. Discontinuation of the monitoring program will result in decertification.

This process of certification testing is modeled after practices in civil aviation where aircraft are certified for release into revenue service after only a few thousand hours of test flights provided a monitoring program is in place that can detect in-service problems. If necessary, the certifying authority may order design modifications or may require that the aircraft be grounded immediately.

4.4. Disposition of Application

It is the responsibility of the applicant to submit a voting machine that meets all criteria necessary for certification. In fact, the applicant is required to attest that with the submission. The assumption is therefore that any application will be approved and the machine be certified as requested.

As a rule, therefore, there are only two possible outcomes of the certification process:

- The machine will be declared fit for use in elections, or
- It will be rejected.

Modification of a machine after certification will not be permitted. Any modification will start a new certification process. Elements of previous processes may be used only if it is clear beyond doubt that they are not affected by the modification. Demonstrating that is the responsibility of the applicant.

5. Meeting Reliability Requirements of the Precinct-Level System

The present paper is focused on the voting machine. Our analysis only includes failures that originate with the voting machine. Any failure of a voting machine will affect the precinct-level voting system. We have shown that such a failure has to be considered critical if it leaves the precinct with an insufficient number of machines.

Protection against machine failures leading to a critical a critical failure of the precinct system comes from two directions:

- Prevention of machine failures
- Keeping spare machines at the precinct.

Both mechanisms need to be considered in achieving an overall optimal precinct system. Although the economy of the situation will be the final judge of what is optimal, it appears that, as described in Section 2.3, providing one spare machine for each precinct will be all that is necessary for most precincts.

It is recommended that separate sets of guidelines be developed that would address the entire precinct-level voting system and the regional voting system, and define reliability and other requirements for them.

6. The Current State of Voting Machines and Implications of a Transition to the New Reliability Requirements

Voting machines in use today were designed to very different requirements than those defined in this paper. The notion of critical failures is absent from these requirements. It is accepted that the inner workings of a voting machine are protected by trade secrets and not subject to inspection. The software driving the voting machines and integrating them into the "voting system" is stored as source code and updated as the operating systems are updated. Software functions are not limited to driving voting machines but tend to interact with the larger voting system at the precinct and regional level, making them vulnerable to accidental or intentional manipulation.

It can, therefore, not be expected that any of the voting machines in use today or in the production program of vendors meet the reliability requirements defined here. It is unlikely that any machines currently offered can be modified easily to meet the new requirements.

The reliability requirements defined in the present paper will lead to voting machines that will be significantly less complex and less expensive than voting machines being offered today. They will lead to a situation where, in a typical precinct on a typical voting day, no machines will break down, and there will be no doubt about the validity of the vote count. Barring the occurrence of failure modes that could not be recognized with the state of the art at the time a voting machine is built, and barring human error in the performance of the functional failure analysis, there will be no need to modify or otherwise disturb voting machines between elections.

Key to a successful development and implementation of voting machines that meet expectations is to maintain the simplicity and transparency of voting machine functionality that is defined in the present paper. The new guidelines and any laws and regulations that govern the conduct of elections need to clearly and unambiguously define a "voting machine" as the physical entity that is bought from a vendor to accept, record, and report votes cast on it. No other functionality can be expected by it, nor must it posses the capacity to perform such other functionalities. Such additional functionality can instead be assigned to the "voting system" where it can easily be accommodated without jeopardizing the confidence in election results. Any attempt to pack additional functionality into a voting machine itself will jeopardize the reliability of the voting machine and may impact the credibility of the voting system in which it is embedded.

The voting machine or an attached unalterable recording device as defined in the present paper is suitable to serve as the primary record of the vote. It will be possible for voting machines to meet the high burden resulting from that only if laws and regulations actually prescribe it as the primary record and impose severe enough penalties for tampering or negligence in handling or maintaining voting machines. Laws and regulations need to stipulate that the record of a vote created by a voting machine be maintained in a verifiably unaltered state until any deadlines for recounts or other time spans specified by laws or regulations have safely expired.

Absent strict laws and regulations, it will be difficult to develop the proper understanding of the potential improvements that voting machines adhering to the requirements formulated in this paper can provide.

A transition to new voting machines that comply with the reliability standard developed in the present paper will be painful and expensive. It will require replacing machines, many of which are relatively new, with a new generation of machines that do not currently exist. The price will be enormous. Only a policy decision made at the political level will be able to determine if the improvement in the credibility of the voting process will justify this cost.

In framing this decision, the political leadership might look for guidance at the experience of the airline industry where an analysis procedure similar to what has been used for the functional reliability analysis in the present paper is credited with a transformation of the industry from one of the most hazardous and expensive forms of travel to the safest and one of the least expensive forms. Key to that transformation was recognizing that a different level of performance is attainable, and that the ultimate cost of the better performing system would be lower. An important part of it was the fact that strict laws supported the will for change.

6.1. Demonstrating the Feasibility of Building Voting Machines to meet the New Reliability Requirements

Voting machines are purchased and used in the center of the political process of our democracy. To most members of this community, the notion of analyzing and designing voting machines following processes used for airliners may appear surprising. It might appear impossible to them that these processes could really lead to the radical improvements that we claim can be achieved in terms of reliability as well as cost. Since this kind of change is outside the envelope of experience for most members of this community, it appears that the most effective way to convince them of the validity of the proposed approach is through a demonstration.

A demonstration would follow the lines spelled out in this paper and define, design, and build a prototype voting machine. The machine would lack the finish of a commercial product, but otherwise would work exactly like a usable voting machine. In particular, it would exhibit the reliability performance proposed in the present paper.

The prototype would demonstrate that:

- A machine can be built to the specifications defined in this paper with a modest effort and in a time of months rather than years.
- The proposed metric can be applied with ease and will obtain the desired result.
- All certification requirements defined in this paper can be met without imposing undue hardship on the applicant, or causing undue delay.

- The machine can be used in simulations of the actual voting environment and pass its part of the specified volume test.

Experience with the design, development, and operation of the prototype could guide the evolution of new generations of voting machines. The cost of developing the prototype, if the project is properly managed, would pale in comparison with the savings that could be realized if voting machines modeled after the guidelines would be purchased instead of current-generation voting machines.

7. Conclusion

In this paper, we presented the result of a complete functional failure analysis of a generic voting machine. We demonstrated that it is possible to design a voting machine that can meet reliability standards that are comparable to those met by commercial airliners.

We defined as critical failures those that threaten the validity of the vote, and found that their occurrence can be excluded or limited to very low probabilities. Prerequisites for this are that the design of a voting machine meets certain requirements. We defined these requirements from the point of view of reliability. However, these requirements are not strictly limited to reliability considerations, but rather impact most requirements formulated for other purposes throughout the guidelines.

We also looked for failures that do not affect critical functions. We found that there are few, and that it should be possible to keep them at a low probability of occurrence. Consequently, we found that there is no need to provide a maintenance capacity during the voting period for the voting machines. Rather, by keeping one spare voting machine at every precinct, it should be possible to keep the probability of critical interruptions of the voting process to practically zero.

The metric that we have defined for the voting machines is the set of probability statements for critical and noncritical failures that is the outcome of a functional failure analysis. Obtaining this metric requires performance of a functional failure analysis. The acceptable limits of failure probabilities are zero or near zero for critical failures, and very low values that have to be determined through economic analysis for noncritical failures or otherwise limited by the certifying authority.

The failure probabilities obtained through the functional failure analysis are validated through testing of components and parts. Test results obtained through certification processes for commercial parts or components can be used. We believe a whole system test to conclusively verify the overall failure rate of the voting machine is not necessary. Such a test would require more time than can be justified. It would also be very expensive. Instead we call for a limited volume test that is designed to validate the findings of the component-based analysis, and continuous monitoring of voting machine reliability in actual operations. Information from this monitoring process needs to be analyzed. If necessary, it will be used as a basis for developing modifications of the voting machines.

We have also defined a process by which voting machines can be certified for all the requirements that pertain to reliability. Like the requirements we defined, the certification process for reliability impacts certification for most other functions defined by the guidelines.

To arrive at a consistent set of requirements for all topics covered by the guidelines, it will be necessary to harmonize all requirements defined here with those that emanate from all other groups working on the guidelines.

Implementing the requirements defined here will not be easy. A new generation of voting machines has just been deployed that do not meet the requirements defined here and for which it is unlikely that they can be modified to do so. By calling for simple and well isolated voting machines, the requirements defined here also, in some ways, go against the current trend. That trend tends to pack voting machines with ever more functions, mostly of election management, and increases the complexity beyond a point where integrity and reliability can be assured for a reasonable cost.

The present recommendations also go against the common notion that in order to improve performance (like reliability), it is necessary to increase the investment. In fact, the experience of airline maintenance shows that precisely the opposite may be true. Better-performing systems can be significantly less expensive, provided the requirements are well defined.

A final obstacle that might need to be overcome is that the election community and the public at large has gotten used to the fact that voting machines are neither reliable nor trustworthy, and therefore, would be satisfied with an incremental improvement over the current performance. The argument has been made that old-fashioned paper ballots are not infallible either. That may be true. However, why would one want to introduce technology if it does not lead to real improvement? Wouldn’t that just be an investment without a return, and an unnecessary complication of a process that is essentially very simple?

In this paper, we have shown that there is no reason to be satisfied with less than perfect. We suggest that to prove this point it may be desirable to design and build a prototype voting machines that will demonstrate that the reliability requirements formulated here are achievable at a low cost. Such a prototype could be completed before the time the next version of the guidelines is scheduled for publication.

DISCUSSION DRAFT

8. References

Etschmaier, Voting Machines: Critical Issues for Formulating Reliability Requirements, August 2006

Technical Standards for Gaming Devices and On-Line Slot Machines of the State of Nevada