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: QUALITY AND CONFIGURATION MANAGEMENT REQUIREMENTS

October 2006

1. Introduction

The notion of “quality” is one of those constructs the meaning of which might be intuitively obvious, but which raises more questions the closer it is examined. In the original meaning, the “quality” of an object simply refers to certain attributes of the object. In the context of quality assurance, “quality” refers to positive values of certain attributes. Identifying those attributes, especially exhaustively listing all of them, and defining criteria for these attributes for the object to be considered as possessing “quality” proves to be an elusive proposition in most circumstances.

Clearly, there is a need to differentiate between the quality of a product and that of a particular specimen of that product. One may define tolerances on dimensions of parts that make up a product, or on performance parameters, and judge a specimen of the machine as meeting quality requirements if all dimensions and parameters are within the specified tolerances. For a product to be considered a quality product, it is necessary for all specimens of that product (or an overwhelming number of them) to meet the quality requirements. However, this is not a sufficient criterion. Even when reliability is included as a performance parameter, a product may meet all tolerance limits and still not be considered being a “quality product.” It is this elusive residue of attributes that makes the notion of quality so difficult to use in a vendor-customer relationship.

Ideally, there should be a way to define for any product a set of attributes that the customer wants and the vendor provides. Any product from any vendor that possesses these attributes will meet the customer’s requirements. The customer is then, e.g., free to purchase the product from the vendor who offers the most favorable conditions. Upon receiving the product, the customer would evaluate it for these attributes and accept or reject the product.

This is indeed the situation with many “commodity products.” It is what many procurement processes aspire to, and it is a central element of the rules of the World Trade Organization (WTO).

The difficulty arises when products represent reasonably complex systems that are on the forefront of technological developments. Evaluating one particular product specimen for compliance with the product design is exceedingly difficult: checking parts tolerances is not possible without tearing down the product; because of the large variance of product operation and environment, evaluating the performance through statistical analysis of product tests with any degree of statistical confidence may prove to be too expensive and time-consuming.

In the evaluation of a product design, one encounters the same problem. Even though the resources available for this purpose are significantly greater than those for testing one particular specimen, what is required to arrive at a meaningfully robust conclusion may still exceed them.

Since the second half of the 20th century, it has been generally recognized that some of the elusive quality attributes of products may be gauged by the process through which the product is designed, developed, and manufactured. Producing a quality product requires a quality process. While "quality control" (and "quality assurance") had long been standard tools to assure that manufacturing plants deliver products that are true copies of the design, this function was considered of interest to the manufacturer in order to avoid the high cost of rejects. Now it is recognized that it is as important to the customer that the products they are buying are the result of quality processes. And it is not just the manufacturing process that is relevant, but also the processes employed to design and develop the product, as well as the processes of marketing and customer support.

The entire series of standards identified as the ISO series 9000 provide a framework for this new approach to quality. In particular, the ISO 9001 standard covers the entire range of issues that all contribute to the ultimate "quality" of a product.

Faulty designs or faulty parts may be recognized in the design, development, or manufacturing process. The temptation might be to "fix" the problem through improvisation. "Patch" or "shim" or "workaround" are some of the terms used to describe these solutions. While in the manufacturing stage, they might be applied to one product or a small number of products; in the design phase, they would affect an entire series or product line.

Products "fixed" in this way may pass an acceptance test. After all, that is the objective of the fix. But their performance in productive operations would not meet expectations. The product would then be regarded as being of inferior quality. Justifiably, the attribute of inferior quality is typically attached to the brand. If a brand uses processes of design, development, manufacturing, and distribution that permit poor quality for one product, the same processes can be expected to produce equally poor quality in other products.

Of course, quality always needs to be seen in the context of the intended purpose of the product. Inappropriately low quality is regarded as "junk" while inappropriately high quality may be viewed as "gold plating," since it may raise the price to levels that cannot be justified for the intended use of the product.

The concept of quality reaches beyond the processes of design, development, and manufacturing:

- Through the marketing and sales process, a vendor takes on significant responsibility for matching a product to a perceived need or intended use by a customer. Inappropriate tactics in this process may lead to a situation where a product is put to a use for which it is not suitable. This may lead to poor quality performance of a product that, in its intended applications, possesses attributes of highest quality.
- After delivery of the product to the customer, the product continues to require support from the vendor in the form of technical assistance for maintenance and repair, and delivery of spare parts. The manufacturer also needs to observe the in-

service performance of the product to identify unanticipated patterns of behavior and to provide remedial actions should the behavior be unacceptable.

After delivery, it may be necessary to know the identity of key components as well as the manufacturing history of the product. After the product has been in service for some time, it may also be important to know any problems (service difficulties) that the product experienced, any corrective actions taken to remedy these problems, any modifications to the product, and any parts that replaced original ones. This process, known as configuration management, is the responsibility of the operator. However, the customer support function of the vendor will play a critical role in it.

Configuration management is an important part of managing the life cycle of technological products. Select components and parts, in addition to their name and part number, are given individual identities in the form of serial numbers. Records are kept on each one of these individual components or parts. This information may include:

- The current location ("stored as a spare," "included in a defined product," "awaiting or undergoing repair or maintenance work," "discarded");
- The history of past locations;
- The history of usage, failures, diagnoses, repairs, and maintenance actions; and
- The manufacturing history (batch, unit, process, location, …).

A configuration management system defines what information is collected at what occasion, and how it is processed and used. It defines the standard for entering information into the system, in particular requiring identification of the person entering the information.

Knowing the manufacturing history might give assurance that a part is genuine rather than an "unauthorized" imitation. It might also help diagnose problems if it is known or suspected that a particular manufacturing process or location may lead to a higher probability of a certain type of failure. Knowing the manufacturing history might help identify such problems and lead to a reexamination of the manufacturing process. Knowing the location of all components might help locate those that might be affected by a particular manufacturing problem. Knowing the history of usage, failures, diagnoses, repairs, and maintenance actions might help identify bad components that, e.g., repeatedly visit the shop with the same problem.

A well-defined configuration management system also may help delineate liability between a vendor and customer and provide a solid basis for warranty claims.

2. ISO 9000/9001

Starting from a British standard, the International Organization for Standardization (ISO) has developed a series of standards to provide a uniform definition of quality management, and to help a customer assess quality practices of a supplier or potential supplier. The premise is that a supplier who employs quality processes throughout the operation will be more likely to consistently produce quality products or services. The customer will be reassured by a supplier who has a similar management philosophy, and uses quality processes not just for the manufacture of goods or delivery of services, but also in the design and development, as well as sales and post-sales support. Similar to what is the practice in Japanese management, the standard assumes that the relationship between a customer and supplier extends well beyond the purchase of a single item at one single time.

Two standards are of interest to the project at hand:

- ISO 9000, which contains the definition of terms and of the general principles of quality management.
- ISO 9001, which identifies all aspects of an organization and its processes and procedures that are relevant to quality management, and defines objectives that have to be met by each of them.

The definition of the standard is generic. It can be applied to any business, industry, or service organization. In very few instances does the standard define more than the title of specific requirements that have to be met; but it is clear from the sum of all titles and the statement of objectives what would meet and not meet the requirements. E.g., under the heading of Resource Management, the human resources section states that,

> *"Personnel performing work affecting product quality shall be competent on the basis of appropriate education, training, skills and experience."*

Under the heading "competence, awareness and training" in the same section, it requires that

> *"The organization shall*
>
> *a) determine the necessary competence for personnel performing work affecting product quality,*
> *b) provide training or take other actions to satisfy these needs,*
> *c) evaluate the effectiveness of the actions taken,*
> *d) ensure that its personnel are aware of the relevance and importance of their activities and how they contribute to the achievement of the quality objectives, and*
> *e) maintain appropriate records of education, training, skills and experience."*

The standard requires the systems approach, is process-based, and requires the involvement of all people in the organization, including top management. In fact, it requires that top management assume and maintain a leadership role in the

implementation and maintenance of quality in the organization. The standard emphasizes clear and transparent documentation of all activities that can be audited, and factual decision making throughout. It demands continual improvement, a customer focus, and mutually beneficial supplier relationships.

The teeth of the standard are in the requirement that every organization develop a "quality manual" that in turn may refer to other documentation requirements, and that the entire quality process is certified. Certification occurs on the basis of audits. Three levels of audits are defined for the certification:

- *"First-party audits."* Such audits are conducted by, or on behalf of, the organization itself for internal purposes. They can form the basis for "self-certification," i.e., an organization's self-declaration of conformity with the standard.
- *"Second-party audits."* Such audits are conducted by or for customers of the organization.
- *"Third-party audits."* Such audits are conducted by independent organizations and result in "certification" or "registration" of conformity.

For the purpose of assuring quality management of voting machine vendors, only the second- and third-party audits would be acceptable. A second-party audit would require that the certifying agency retain the capability to perform such audits. It appears unnecessary to develop this capability, since there already exist numerous organizations that can perform audits in a reliable and trustworthy manner. Quality control over these organizations is provided by the ANSI National Accreditation Board (ANAB), which operates an accreditation service for ISO 9001, ISO 14001 (defining environmental management systems), as well as for a number of industry-specific requirements.

3. Relevant provisions in VVSG2005

3.1. Quality Assurance

Section 8 of VVSG2005, Quality Assurance Requirements, defines Quality assurance as *"a vendor function that is initiated prior to system development and continues throughout the maintenance life cycle of the voting system."* (Section 8.1, Scope). It leaves a vendor free to design and implement any *"quality assurance program [that will] … ensure that the design, workmanship, and performance requirements are achieved in all delivered systems and components"*. (Section 8.2, General Requirements). Carrying out quality assurance tests is the responsibility of the vendor who is required to provide test data and test reports to the test lab as part of the national certification process, as well as, upon request, to the purchaser. (Section 8.4, Responsibility for Tests)

The vendor is required to *"select parts and materials … and components according to their suitability,"* and, *"if needed, design [and perform] special tests to evaluate the part or material under conditions accurately simulating the actual voting system operating environment."* They are required to *"maintain the resulting test data as part of the quality assurance program documentation."* (Section 8.5, Parts and Materials Special Tests and Examinations)

With each system or component delivered to the test lab or to the jurisdiction, the vendor has to deliver a *"record of tests or a certificate of satisfactory completion of conformance inspections [that] … ensure the overall quality of the voting system and components."* (Section 8.6, Quality Conformance Inspections).

The quality assurance program is required, at a minimum, to:

a. "Include procedures for specifying, procuring, inspecting, accepting, and controlling parts and raw materials of the requisite quality
b. Require the documentation of the hardware and software development process
c. Identify and enforce all requirements for:
    i. In-process inspection and testing that the manufacturer deems necessary to ensure proper fabrication and assembly of hardware
    ii. Installation and operation of software and firmware
d. Include plans and procedures for post-production environmental screening and acceptance testing
e. Include a procedure for maintaining all data and records required to document and verify the quality inspections and tests." (Section 8.2, General Requirements)

VVSG2005 defines the scope of quality assurance broad enough so that it can include all functions that are required to assure that a quality product is delivered on a consistent basis. However, it does not refer to any standard the quality assurance programs are required to comply with, nor does it contain any mechanism according to which a vendor program might be certified.

Presumably, the recipients of test data will impose some standards on the data and refuse to examine a voting machine the documentation for which does not meet these standards. If this does impose something akin to a certification of the vendor quality assurance program, it comes at a stage after the program has already run its course. Retroactively correcting it would be extremely difficult and costly. The situation is further complicated because commercial pressure on the vendor to deliver promised products, as well as business considerations of the testing lab and looming election deadlines might force acceptance of conditions that otherwise would not be acceptable.

3.2. Configuration Management

"Configuration management is defined as a set of activities and associated practices that ensures full knowledge and control of the components of a system, starting with its initial development and progressing through its ongoing maintenance and enhancement." (Section 9.1, Scope)

VVSG2005 describes the configuration management functions only in terms of their purposes and outcomes, and leaves specific steps and procedures to the vendor to select. However, it does not contain any mechanism by which the procedures for configuration management might be certified.

Similar to the requirements for quality assurance, vendors are required *"to submit these procedures as part of the Technical Data Package for system certification."* State or local election legislation, regulations, or contractual agreements may add additional requirements. The EAC and state and local election officials are given *"the right to inspect vendor facilities and operations to determine conformance with the vendor's reported procedures and with these requirements."* (Section 9.1, Scope) As was pointed out in the discussion of quality assurance requirements, it would be very difficult to require changes in the procedures at that point.

VVSG2005 requires two types of configuration audits as part of configuration management: *"Physical Configuration Audits (PCA) and Functional Configuration Audits (FCA)."* (Section 9.7, Configuration Audits) It appears that these audits are part of the quality assurance function and would be better placed there. They would seem to be part of the quality checks that are performed at critical stages of the design and development processes, as well as the final quality check in manufacturing. They should be the responsibility of the vendor.

Preserving Configuration Management Resources, as addressed in Section 9.8, is part of the enforceable commitment for product support throughout the life cycle of sold voting machines. It should be addressed with all other commitments that need to be demanded of a vendor, and does not belong in a section on configuration management.

3.3. Summary

VVSG2005 contains many of the provisions that are required to assure that voting machines put into operations meet what should be expected of them in terms of quality. It also defines a process of configuration management that addresses most of the elements that need to be part of an effective program. However, the provisions lack specificity, especially in the criteria by which a vendor program is being judged to be acceptable. There is no formal step to approve ("certify") a vendor program, and any evaluation comes at a stage when it is all but impossible to make any corrections.

A thorough reexamination of the issue of quality assurance and configuration control appears necessary to the formulation of requirements that will lead to voting machines that will perform as should be expected.

In this report, we are addressing the basic issues and defining a framework for future versions of VVSG. The framework bears on many other aspects of VVSG and does suggest some modification of current practice. A thorough discussion within CRT and TGDC, as well as with communities representing vendors as well as users (jurisdictions) of voting machines, will be necessary to assure that it fits into the policy direction and the overall schema of new guidelines. Future reports will deal with questions of implementation of and transition to the new framework, and provide a draft for the text to be included in the new guidelines.

4. A Framework for Quality Assurance and Configuration Management of Voting Machines

In this section, we will translate the general concept of quality assurance and configuration management to procurement and operation of voting machines. We will briefly describe the definition and key features of a voting machine that emerged from our previous work. Based on that, we will define a framework within which requirements of a vendor in terms of quality assurance and configuration management procedures can be defined. The framework will also help define the complementary processes that a customer (jurisdiction) needs to implement as a condition for the vendor programs to be effective.

Figure 1 recapitulates our general description of quality assurance and configuration management in terms of voting machines.

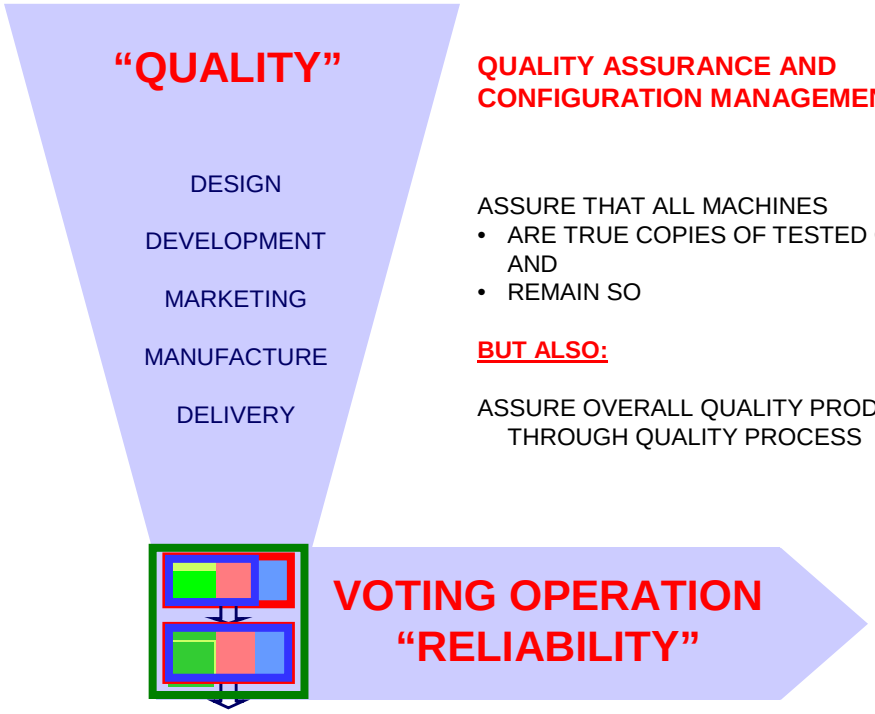

Figure 1
Quality Assurance and Configuration for Voting Machines

Our analysis of reliability requirements [Etschmaier 2006a and 2006b] led to the definition of a voting machine as a secure repository of the original vote cast by voters. This voting machine can hold the inalterable record of the vote as long as required by law, and serve as the final fixed point in any recount. It feeds into the higher layers of the

voting system but does not "interact " with them. Figure 2 provides a conceptual overview of this voting machine.

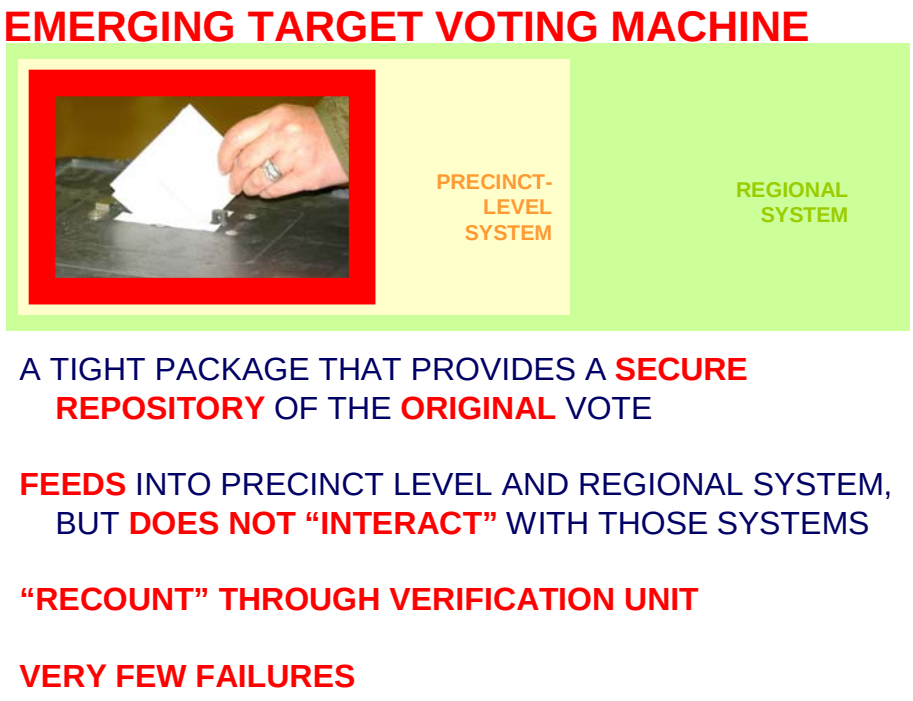

Figure 2
Conceptual overview of the voting machine

The important aspects of the voting machine are that:

- It is a clearly defined product with clear boundaries;
- It consists of hardware, software, and data storage elements;
- The hardware and software are designed not to change over the life of the machine;
- Data held in the storage devices only change in narrowly defined ways and without penetration of the perimeter of the machine;
- It can be sealed after delivery to the "customer" (e.g., a state voting commission);
- It requires no routine maintenance, and its functions can be diagnosed from the outside; and
- Data can be entered and accessed without disturbing the perimeter of the machine.

Figure 3 shows a generic model of a voting machine. The model is neutral as to the technology used to build an actual machine. The division of the machine into components may or may not serve as the blueprint for the structure chosen. The purpose of showing this model is to demonstrate feasibility of a voting machine that is simple, yet will not fail during a typical election cycle. Any real voting machines may be based on a different breakdown into components.

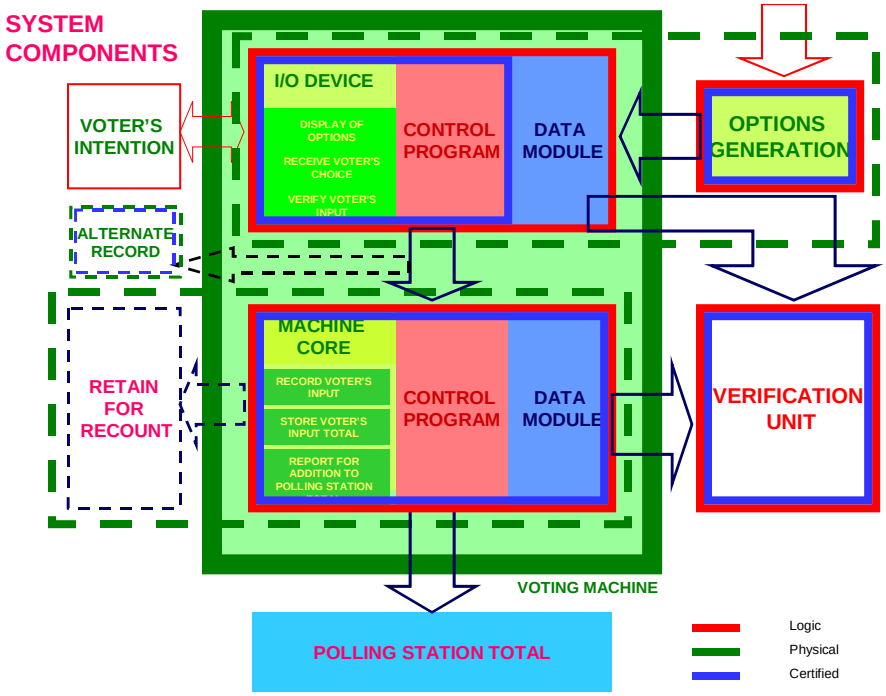

Figure 3
Components of a Generic Voting Machine

This voting machine can be developed and produced in an environment where there are precisely defined rules and requirements, where the required functions and their criticality are precisely defined, and the rules are enforced unambiguously. We defined the requirements on reliability in a previous paper (Etschmaier 2006b). The clarity with which these are translated into regulation and enforcement is as important to obtaining quality voting machines, as is the definition of quality and configuration management processes. Only unambiguous rules and regulations, and strict enforcement can lead to satisfactory results.

Part of these rules concerns what we defined, in our first report (Etschmaier 2006a), as the various layers of the voting system – election management, and the operation of a

polling place. We urge that these issues be addressed with urgency to provide an overall system of voting that will re-earn the confidence and trust of the population.

Figure 4 shows a framework for a combined quality assurance – configuration management system that cuts across the boundaries between the vendor and the customer.

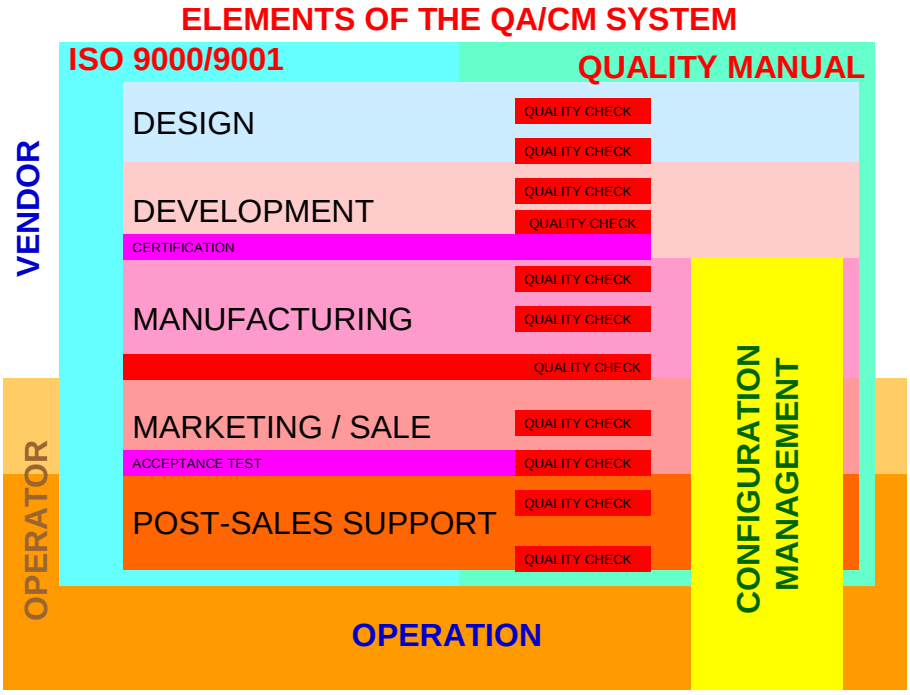

Figure 4
Framework for a combined quality assurance – configuration management system

The framework is based on full certification to the ISO 9000/9001 standard that defines requirements in generic terms. In order to translate these into concrete processes and procedures at the vendor level, it is necessary to develop a comprehensive "quality manual." These two documents cover the entire range of quality issues throughout the vendor operation: design, development, manufacturing, marketing and sale, and post-sale customer support. A customer who insists on quality products will want to verify that these are in place and observed strictly, that there is an enforcement mechanism with sufficient powers and independence, and that they are able to inspect the facility and operation, as they feel necessary. A large customer may want to "certify" the vendor operation and facility that it complies with their expectations. A vendor who designs and develops a product, such as a voting machine, that is used only by one or one coordinated group of customers, may expect that the certification, if it is to be issued, is issued before they begin investing in the design and development process.

The figure also shows a bar that represents configuration management. This process really starts when the parts and components become a reality during the manufacturing process, and are assembled into a voting machine. Ideally, the vendor-based part of configuration management should seamlessly lead into the customer-based part upon handover of the vending machine. For this to be possible, the two parts have to be compatible in structure and format. The customer may make a compatible configuration management system a condition of purchase. As is the case with the quality assurance program, the vendor will want to be sure his or her program meets customer expectations before committing any resources toward producing machines. However, since the vendor part of configuration management is comparatively small and uncomplicated, a formal "certification" may not be necessary. The customer may simply spell out the rules they expect to be observed, and access to what information they will want to get in order to verify compliance.

For the customer, configuration management starts with the beginning of purchase negotiations, when the customer needs to examine existing procedures. It continues from the purchase decision through the start of operations, since the customer needs to get the system ready for the new product. The real operation of the configuration management system, however, does not begin until the delivery of the first voting machines.

4.1. Elements of the Quality Assurance Program of a Vendor of Voting Machines

The quality manual details the quality process for a vendor within the framework of ISO 9000/9001. Quality assurance covers the entire process from design and development to manufacturing and post-sales support, and also includes marketing. In each one of these steps, quality checks will be performed. The quality manual defines the criteria according to which quality checks need to be placed into each step and the format for each step. Criteria and format of the checks will be different for each step. The actual number of these checks, their placement in the process, and the definition of the work that is to be completed before each check, will be determined by the project plan for a specific project. An overview of the content of the quality manual is shown in Figure 5.

QUALITY MANUAL

DETAILS PROCESS WITHIN FRAMEWORK OF ISO 9001

SPECIFIES PROCESS STEPS AND QUALITY CHECKS

DEFINES AUTHORITY AND RESPONSIBILITY

DEFINES EXCEPTIONS REPORTING REQUIREMENTS

Figure 5

Overview of Content of Quality Manual

For the design and development process, quality checks will determine that the project has progressed to the state it is supposed to be in, that all issues that were supposed to be addressed were addressed, and any questions and problems resolved. One possible form of these checks is the peer review by company personnel that was not involved in the reviewed project, or at least the process step. The manual defines the authority and responsibility for these checks and the conditions under which the project may move forward.

At the end of the development process the final quality check by the vendor, if passed, is followed by an initial production run, product testing by the vendor, and, if successful, the certification evaluation and testing by the certifying agency. An overview of a quality check in the design and development stage is given in Figure 6.

CHECK POINTS IN DESIGN AND DEVELOPMENT STAGE

- COMPLETE EVALUATION OF PROJECT BY PEER GROUP
- NUMBER MAY BE DIFFERENT FROM WHAT IS SHOWN
- EXTENT SPECIFIED IN PROJECT PLAN, BASED ON QUALITY MANUAL
- PASSING REQUIRED BEFORE CONTINUATION TO NEXT STEP
- ITERATIONS BETWEEN CHECK POINTS DURING DESIGN AND DEVELOPMENT PHASES

Figure 6
Quality check in the design and development phase

While the quality checks in the design and development stages address a type of voting machine, in the manufacturing process, they concern individual specimen as they are produced. Quality checks will determine that parts, components, and the final assembly of a machine conform to the design. The quality manual spells out the rules and criteria for determining at what stages in the process quality checks need to be performed, and the scope of these checks. It provides rules to determine who is responsible for each check, and who is authorized to reject a product or stop production. It also spells out rules for documentation, certification, testing, and other evaluation of parts and components, made in-house as well as purchased.

The manual spells out rules for recording and reporting exceptions in the manufacturing process, and defines the circumstances under which exceptions have to be reported to the configuration system as well as the processes used to evaluate exception reports and to respond to unacceptable situations.

The manual also defines responsibility for the different aspects of the quality process, as well as the authority to correct exceptions that were identified through it.

As the final step in the manufacturing process, the vendor will perform a pre-delivery quality checkout of the voting machine. This check will provide assurance that a machine that is delivered to the customer will be as designed and specified, and operates accordingly.

The post-sales support is probably the most important requirement for a technological product to perform as a quality product. The vendor support includes advice in the use of

the product, as well as technical support in identifying and analyzing exceptions and failures of voting machines, and developing corrective measures.

Our report [Etschmaier 2006b] defines a requirement for reliability performance monitoring. It defines a monitoring process in the form of a feedback loop in a system in 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."*

The quality manual will define the vendor standards and capabilities to provide post-sales support and to support the reliability performance monitoring and design improvement process. The new guidelines will include precise requirements.

The report [on reliability requirements] also requires

> *"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."*

While this requirement may be viewed as part of the process of vendor certification defined later in this report, it may neither be necessary nor practical to do so. Rather, this clause should be part of the sales contract.

It appears to go against much of the conventional wisdom for a customer to be concerned with the quality of the marketing and sales process of a vendor. However, if the vendor-customer relationship is to be based on long-term trust that is required for a quality operation of technological products, it is very important that marketing and sales be conducted in an honest and fair manner, and that all materials provided to the customer are accurate and correct.

The customer responsibility in the quality process is not included in the vendor's quality manual. It is limited to the acceptance test the customer will perform when they receive a machine. This test will mirror the pre-delivery checkout that the vendor performed before shipping. With these two tests in place, there should be reasonable assurance that any

machine that enters service is in operational condition. An overview of the acceptance test is given in Figure 7.

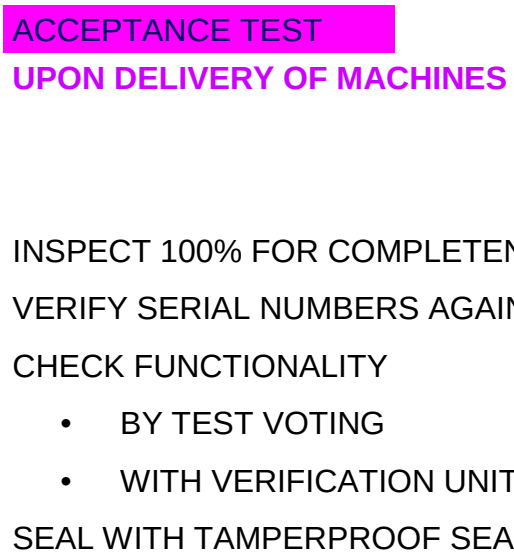

Figure 7
Acceptance Test by the Customer

The acceptance test is done on all machines as they are received. It is performed by a qualified voting machine technician who works for, or on behalf of, the customer. A description of the qualifications of the technician will be provided in Section 4.3.

The acceptance test will include:

- An examination of the configuration management document that the vendor provided with the voting machine, and a verification of the serial numbers;
- An complete checkout of the functionality of the machine by test voting according to a predetermined protocol; and
- A checkout of the functionality by means of the verification unit.

Upon positive completion of the acceptance test, the technician will seal the machine with a tamperproof seal that bears their identification and the date. The configuration management file will be entered into the database for active voting machines. The acceptance test, therefore, is at the intersection between quality assurance and configuration management. It is part of both processes.

Machines that fail the test will be returned to the vendor. A record of the exceptions together with the serial number will be entered into the exception report.

4.2. Elements of the Configuration Management Program of a Vendor of Voting Machines

Configuration management is the complement to quality assurance and provides the basis for quality processes at the operator of voting machines. As mentioned above, it starts with a positive acceptance test of a voting machine that is received from the vendor. It is mostly a function that exists at the customer, with the vendor providing some basic prerequisites.

In this section, we will describe the key elements of a configuration management program. The basis of configuration management is the identification that is attached to individual voting machines, their components and parts, and the documentation that is being kept about. We will first define the identification and documentation requirements before describing the most important processes. We will conclude by introducing the position of voting machine technician as the key person to assure the integrity of voting machines in customer inventory.

Figure 8 summarizes the identification requirements for a configuration management system for voting machines.

Every voting machine has a unique serial number that is shown on an identification tag that is attached to the main body, and is tamper resistant and difficult to remove. In addition to the serial number, the tag contains the following information:

- The model identification in the form of a model number and possibly a model name. The model identification identifies the exact variant or version of the machine, and refers to a document that contains all design details, including software versions of the particular specimen.
- The serial number that uniquely identifies the machine, and is in the format used by the configuration management data system.
- Identification of the vendor, including address and contact information for technical service, and vendor certification information.
- Date and number of the type certificate for the voting machine.
- Date of manufacture of the voting machine.

Every component is identified through a component identification tag that is attached to a key part in a visible place. The information on the component tag is similar to that on the machine tag, except that, in addition to the voting machine vendor, it may also identify a manufacturer who may be different from the voting machine vendor.

All parts that play a critical role in the operation of the voting machines are also serialized and identified through a tag that is similar to the component tag.

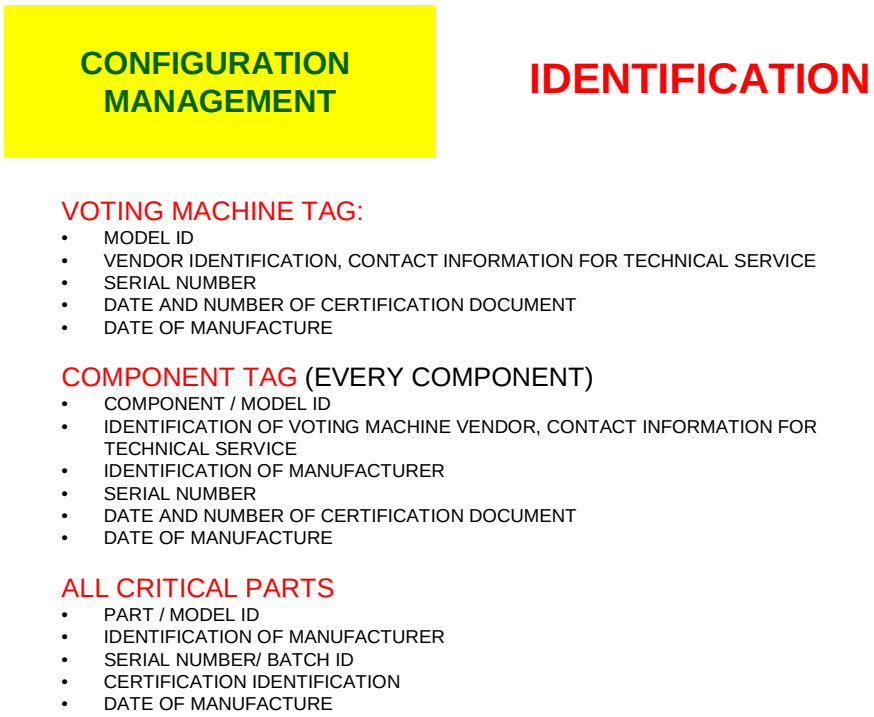

Figure 8
Identification requirements

The documentation kept by the configuration management system consists of the configuration log and the usage log. A summary view is given in Figure 9.

A configuration log is kept of every voting and every serialized component and part. For the voting machine as a whole and components, it identifies all serialized elements included in them. For all serialized items, it contains the complete configuration history as well as the history of exceptions, failures, maintenance actions, and repairs. From the set of all configuration logs, it should be possible to reconstruct the entire history of all voting machines.

The configuration log is kept on an unalterable medium. It is initialized by the configuration data supplied by the vendor. From that point on, it functions like a diary of the machine. Entries are made whenever any change occurs. Every exception and every failure is recorded. Every time the cover is opened for inspection or a repair or maintenance is performed, an entry details what was done, and what component was changed against what other component, as well as any diagnosis of failures or exceptions. The only person authorized to make entries in the configuration log is a qualified voting machine technician.

CONFIGURATION MANAGEMENT

DOCUMENTATION

CONFIGURATION LOG OF EVERY VOTING MACHINE
- ID OF PARTS AND COMPONENTS
- HISTORY OF EXCEPTIONS AND FAILURES
- HISTORY OF REPAIRS AND MODIFICATIONS

EVERY ENTRY SIGNED BY AUTHORIZED PERSON
LOG IN UNALTERABLE MEDIUM

USAGE LOG
RECORD OF BEGINNING AND END OF USE DURING ELECTION CYCLE
EVERY ENTRY SIGNED BY AUTHORIZED WORKER

Figure 9
Documentation in the Configuration Management System

The usage log records the beginning and end of use of the machine during an election cycle. (Other uses, except for maintenance and repair, are not authorized.) The entries are made by the authorized poll workers who start up or shut down the voting machines during the election. The logs serve primarily as a record for recounts, but also are used for trouble shooting of failures.

Figure 10 summarizes some key processes of configuration management.

Attaching and breaking the seal of a voting machine

Every voting machine is enclosed by an enclosure that bars access to all parts and components and assures the integrity of the machine. The enclosure is locked with a seal that is affixed by a qualified voting machine technician. It can only be broken when necessary by a qualified voting machine technician. Attaching and breaking the seal has to be recorded in the configuration log for the machine.

Changing components and parts
Components and parts may only be changed when necessary by a qualified voting machine technician. They may be exchanged only against like ones or against ones that

are certified to be true substitutes that will not change any aspect of the functioning of the voting machines.

Modifications

Modifications are actions that change the functioning of the voting machine. They may be necessary because it was recognized that the voting machine in its existing configuration will not work as expected or will not be as reliable as needed. Modifications can occur through replacement of components by ones with different functionality, or by rebuilding components to different functionality. Any modifications may be made only upon the explicit order of the certifying agency.

Figure 10
Key processes of configuration management

4.3. The Certified Voting Machine Technician

The certified voting machine technician is the key to operating voting machines that are both reliable and trustworthy. They are people who are technically qualified to work on voting machines, have received training in legal and ethical issues of relevance to the operation of voting machines, and are sworn to their duty. An overview of the scope of this position is given in Figure 11.

Concomitant with their responsibility would be the threat of severe criminal penalty for any violation of this trust. It should be examined if existing laws and regulations are adequate or if it would be necessary to craft new ones that would provide for stricter enforcement powers.

The certified voting machine technician is identified through a unique seal that they affix to voting machines that they have verified as working as required. They are the only ones authorized to, when necessary, break a seal of a voting machine. They are required to record any activity they perform on a voting machine in the configuration log. They will also record exceptions and failures. They will monitor the in-service performance of the voting machines and interact with vendor technical staff to diagnose problems, and may initiate the development of solutions. They are not authorized to make any change to the functioning of a voting machine without the orders from the certifying agency.

Figure 11
The certified Voting Machine Technician

4.4. Vendor Certification

As mentioned above, it is in the interest of vendors to have a process in place through which the certifying agency will determine their qualification to develop and supply voting machines for use in elections. Carrying out this process before the start of the

design and development process will make sure that a vendor does not invest resources in a product that they may ultimately not be qualified to produce.

An overview of what such a certification of a vendor would include is shown in Figure 12

Figure 12

Requirements for Certification of Vendor Processes for QA and CM

A vendor is required to have a full certification of conformity with ISO 9000/9001 through a third-party audit performed by an organization accredited by the ANSI National Accreditation Board (ANAB). The certification will include a certified quality manual.

The new version of VVSG may impose specific requirements on the quality manual which may require amendments to the manual. It will also define requirements for vendor responsibilities in the configuration management process. There may be other requirements that will emanate from other parts of the new VVSG. All requirements should be combined into one package and subjected to certification in one process.

When the vendor is satisfied that their quality manual, configuration management process, and processes and procedures defined by other sections of VVSG meet the requirements, they will submit them to the certifying agency. With this they will supply:

- A copy of the ISO 9000/9001 registration certificate;
- A sworn statement that
  - the processes and procedures are actually being followed in their facilities; and

- that they have processes in place to assure that all their suppliers adhere to the parts of the manual that are relevant for them.

The certifying agency will verify that the supplied documents comply with the requirements, and inspect the vendor facilities to verify that the implementation meets the requirements. Upon satisfactory completion of this evaluation, the certifying agency issues a certificate that declares the vendor qualified to supply voting machines.

In addition to the requirements covered by the vendor certification process, Section 4 requires that the vendor provide an "enforceable assurance that the applicant is qualified and financially fit to provide technical support for the machine over its projected service life." The vendor should be aware of it at the point of certification. However, the assurance will not be demanded until the time of sale.

4.5. Other considerations: Environmental quality management

It might be worth to consider requiring a vendor of voting machines to comply with the standard for environmental quality management that is codified in ISO 14000. This standard is often considered a companion to the ISO 9000 family. As we have argued elsewhere (Etschmaier 2006c), a company that is committed to quality cannot be selective in this commitment. Quality is only sustainable if it covers the entire enterprise.

A potential justification for inclusion of this requirement is that demanding adherence to ISO 14000 standard would not be so much of a burden on the vendor as it would merely demand consistency in the implementation of quality management. Irrespective of this, one might also argue that a company that is entrusted with the design and manufacture of a piece that is key to the operation of our democracy should be expected to act responsibly in the use of our key resource, the environment.

5. Operator Roles and Responsibility in Quality Assurance and Configuration Management

This report is addressed to defining requirements of a vendor of voting machines that will assure that the operator receives a quality product and is able to maintain the quality throughout the life cycle of the voting machine. Throughout this report, we have described vendor capabilities, activities, and processes that are a prerequisite for the vendor requirements to be effective. In fact, much of the requirement of configuration management is actually located in the hands of the operator.

Defining requirements from the point of view of the operator would exceed the bounds of this report. Instead, it is recommended to collect all operator requirements and make them part of a volume of guidelines for election management. This volume would complement VVSG in the current scope.

6. Implications on the Design of Voting Machines

An analysis of requirements for quality and configuration management would not be complete without examining if there are design features of the voting machine without which the requirements could not be implemented. There may also be other design features that, while not necessary, might be recognized as desirable.

The single requirement on the design that emanates from this analysis is that the voting machines have a secure closure that can be locked and secured with the seal of the certified voting machine technician. The enclosure has to bar access to any part of the voting machine except for the communication channels that are specifically intended for communication with the outside.

Another consideration that might be added as a design requirement is Energy Star compliance. Energy Star certification is already granted to many products with technologies similar to those in current voting machines. Energy savings that are required for it appear easy to achieve. Requiring them would be consistent with the requirement for ISO 14000 certification.

7. Conclusion

This paper is a first discussion of requirements for quality assurance and configuration management. Like the preceding paper on reliability requirements, it uses an overall systems approach. As a result, we have arrived at many observations that go beyond the scope of the subject at hand. Some of these observations lead to the formulation of requirements that should be considered for inclusion in other parts of VVSG.

There is always more than one answer to a question and more than one solution to a problem. This is certainly the case with formulating requirements for a system that is as complex and used by so many parties as are voting machines and voting systems. We have provided an outline for one solution. A discussion now needs to ensue to formulate the solution that will meet the expectations and requirements of all parties affected by it.

8. References

Etschmaier, Maximilian M., Critical Issues for Formulating Reliability Requirements, August 2006
Etschmaier, Maximilian M., Definition of Requirements, Metrices, and the Certification Process, September 2006
Etschmaier, Maximilian M., Environmental Policy and Regulation, and the Practice of Management: A Call for a Burden Added Tax, The International Journal of Environmental, Cultural, Economic, and Social Sustainability, Volume 1, Number 2, 2005/2006
ISO 9000, Third Edition, 2000
ISO 9001, Third Edition, 2005