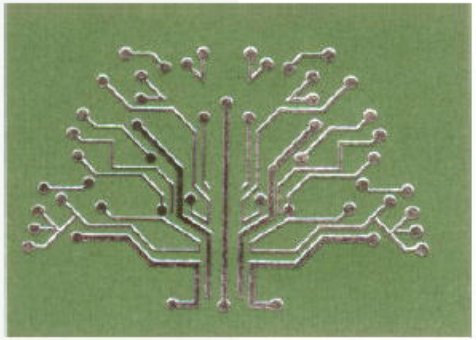

FREEMAN, CRAFT, MCGREGOR GROUP

Voting System Modifications and Constant System Change as Challenges to Future Testing and Certification Programs

National Conference on State Certification
Testing of Voting Systems
June 4-5, 2014
Denver Colorado

Certifications are static. Systems are not.

A certification is confirmation that a specific system conformed with a specific set of standards at the point in time when it was evaluated.

Documentation of certification must include a description of the system's composition.

A good example is found in a recent Wyle Laboratories test report of the Dominion Voting System on the US Election Assistance Commission's Website.

It lists as Deliverables to the customer:

- Five applications
- Seven proprietary hardware items 3 of which are driven by firmware
- Seven COTS hardware items.

Additionally it lists seventy four other hardware and software items necessary to build the system and provide the operational environment.

Change is good.
Change is bad.

Any change, after certification, however small, will degrade the assurance provided by the certification to some degree. The extent of the degradation may be difficult to assess.

Change is necessary for the system provider to insure the integrity of the product throughout its life.

Change is often triggered by external forces such as:

- the supply of system sub-components,
- new security risks and
- changes to user needs.

Change is unavoidable and accelerating

Rapidly changing risks.

Rapidly changing requirements.

Rapid and unpredictable changes in global supply chains.

Acceptance, expectation and accommodation of change:

In the technology industry,

by consumers.

The Future

The Report of the Presidential Commission on Election Administration shows a decided preference for:

- Standards and a certification process that allow innovation in voting technologies,
- Faster and less-costly certification for new products,
- Certifying component (customizable and interchangeable) products and voting systems.

The future, as we see it.

Future decision makers such as legislators, voters and agency heads will not understand or be willing to accept the bias against secured transactions on the internet or the presumption that paper documents are necessary and secure.

Secure distributed systems with mobile devices running on public networks (the internet) will require faster and more frequent changes to mitigate the constantly changing risks in the environment.

How do you know?

The problem for election officials when results are challenged is finding an answer for the question How do you know these results are correct?

"We always do an L&A test…"

Wrong – Competent L&A testing proves the election definition and ballots are correct. Sample size is generally too small to prove system accuracy.

"We use system certified by…"

Great – How do you know?

<u>You must know.</u>

How do you know?

With present systems, jurisdictions must:

- Conduct system validation at system acceptance,
- Track engineering change orders through the life of the system,
- Document their acceptance or rejection and installation of changes to the system,
- Show that the certified system, with approved changes, was used in the election,
- Show that that the election definition and ballots were correctly designed,
- Conduct a competent post election audit.

How do we do this in the future?

We need to take a look outside our own industry.

Our problems are neither new nor unique to our industry.

Other industries with secured systems requiring certification and accreditation include:

- Credit Card Processing.
- Casinos, lotteries, and Pari-mutuel wagering
- Banking
- Healthcare

How can we do certifications in the future that are better, faster and cheaper?

Move independent certification testing into the development process.

If a vendor is developing a product that must be third party certified, doesn't it make sense to apply for certification at the beginning of the project and allow the third party testers to review the work as it is being done?

- Errors in system needs analysis and design can be corrected before any code is written.
- The development process can be evaluated in real time rather than from records of past activity and weaknesses can be corrected when found.

How can we do certifications in the future that are better, faster and cheaper?

Source code can be reviewed and defects can be corrected when found.

Modules can be tested immediately after developers complete, and are satisfied with, their internal testing.

Once the system is ready for release, source code will have already been examined, modules will have been tested for compliance, functionality and security. The independent tester, armed with a high level of knowledge of the system can run through their end to end functional and security testing very quickly.

How can we do certifications in the future that are better, faster and cheaper?

As the system life cycle moves into maintenance and support, patches and planning for future upgrades continue to involve the testers so that patches, when completed are very close to being ready to be rolled out as engineering change orders or versions of the system.

How can we do certifications in the future that are better, faster and cheaper?

Consider requiring the use of trusted suppliers of COTS hardware, software and system components.

- The Open Group has published “Open Trusted Technology Provider™ Standard (O-TTPS) Version 1.0 Mitigating Maliciously Tainted and Counterfeit Products” and begun an accreditation program for compliant companies.
- It provides supply chain best practices for suppliers, developers, and integrators who produce or use COTS hardware and software.
- Other standards bodies are working on variations of such standards.

How can we do certifications in the future that are better, faster and cheaper?

Consider standards for certifying system components that use a common data format and are designed to be used as a component in any voting system.

Evaluate the developer's process so confidence in these processes can become part of the assurance of their products and lower the risk for testers.

Accreditation of the developer's change control and patching process could ease concerns about engineering change orders and the roll out of approved changes to users.

Contact Information

Paul Craft
craft@fcmconsulting.com

Kate McGregor
mcgregor@fcmconsulting.com

Freeman, Craft, McGregor Group
P. O. Box 1717
Tallahassee, FL 32302-1716

Telephone 850-212-8884