Improving Government Certification Testing

Far more than private sector businesses, global government agencies rely on standardization to ensure people, processes, and missions are uniformly focused in their goals. This level of assurance is equally paramount in the communication systems throughout and between agencies. To deliver products that comply with rigorous security and assurance standards, networking and communications equipment vendors must rely on government certification labs.

Lab testing and evaluation are key components of many government certifications. Unfortunately, today's government certification labs are facing increased challenges related to:

- Relevancy
- Efficiency
- Effectiveness

This paper will explore, and make recommendations to address, the policy, process, and overall lab operations issues that are restricting vendors from delivering a comprehensive certified product offering to the marketplace.

Policy

Many labs operate on a 1:1 test to certification policy. This means that a certification is issued exclusively to the hardware and software version tested, and the certification is not valid on subsequent, incremental hardware, or software revisions. For example, a certified product that is going from software release 5.4 to 5.4.1 would have to be retested to be certified. While this may be a safe and conservative approach to certification testing, it results in a policy that radically increases test time and cost, and which ultimately provides a less-than-optimal set of products for customers. This type of policy drives vendors to opt out of certification on certain product sets.

With certain current policies, vendors are unnecessarily forced to make choices on which products to certify, because even though certain modular components on various products utilize the same line cards and modules of other already certified components, the vendor must resubmit each element for testing if any one element is different. This process becomes unmanageable, so the vendors typically decide to only certify on one product, which on average offers more performance or capability than the customer may require.

In many cases of secondary certification, the hardware submitted for testing is similar, if not identical, to the original product. Often the only difference is a processor clock speed, the quantity of memory, or number and/or types of interfaces. Allowing certification by "similarity" would allow labs to increase their effectiveness by increasing the number of products they are able to evaluate with very little additional effort.

Moving to a process of certification by similarity would reduce cost and time, enabling greater customer satisfaction with a higher yield and variety of certified products – many at a lower cost. The U.S. Defense Information Systems Agency (DISA) Joint Interoperability Test Command (JITC) uses a good model. JITC tests the largest, most capable product in a family, and based on the results, it also approves the other (smaller or less capable) products in the family. The same approach is used for line cards and modules. Testing is performed on the card or module with the greatest number of interfaces and other, less capable, cards or modules are also approved.

Clearly, this model requires an overall evaluation of the product to ensure the hardware components and design are the same across all products in the family, or across similar cards/modules, but this can typically be accomplished by reviewing product data sheets and/or additional information provided by the vendor. In this model, if future testing of a new software version on the same hardware is performed, the previous evaluation of hardware similarity can be reused.

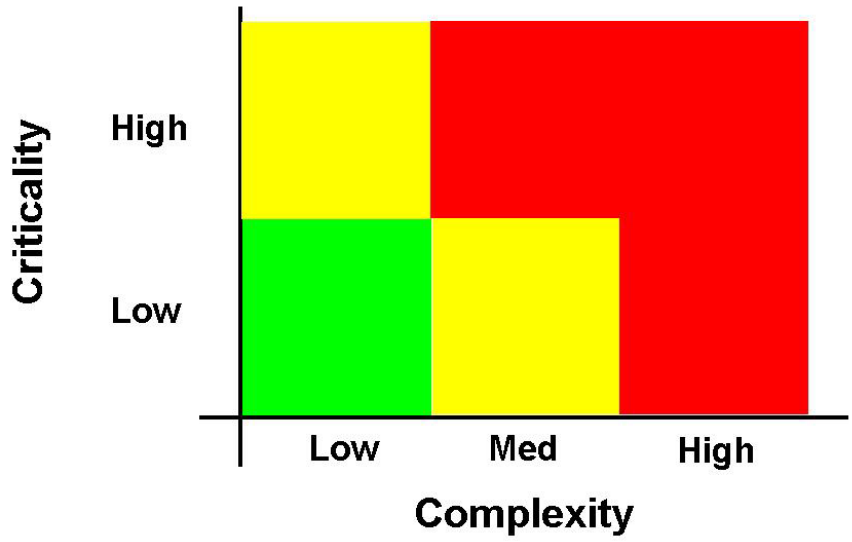
It is not uncommon for vendors to issue multiple software maintenance releases for a product each year. Because of the time and money involved in certifying a software release, vendors do not certify every maintenance release. If one of the maintenance releases has a bug fix that a customer requires, that customer is now faced with the dilemma of having to choose between a certified version of software and one that may have a critical bug fix. Most certifying organizations have a process to address this, but, depending on the number of bug fixes that go into a maintenance release, it may require some level of regression testing.

For LAN equipment, the U.S. Army Technical Integration Center (TIC) evaluation of a software release includes all subsequent maintenance releases. In other words, once the TIC has evaluated a version of software for a LAN product, all subsequent maintenance updates to that software are automatically approved.

Process

The foundation for regression-level testing, and whether it should be required at all for subsequent software releases of an already certified product set, should be based on an equation of criticality and complexity of the product. Criticality is a measure of how critical a particular network element is to the mission. A good example of something that is highly critical is a voice switch, while voice mail would be considered noncritical. Complexity is a measure of how complex a product is. A voice switch is considered highly complex, while a basic firewall product would measure low on the complexity scale. Using these two criteria, a graph such as the one shown in Figure 1 can be used to determine retest criteria for software updates.

Figure 1. Certified Software Retest Requirements – Criticality versus Complexity



Employing a scale, such as the one shown in Figure 1, retest requirements would be based on a product score. For example:

- High score (red) requires certification of every release (with the possible exception of a small patch or small number of bug fixes)
- Medium score (yellow) requires certification of minor releases but **not** maintenance releases
- Low score (green) requires certification of major releases but **not** minor or maintenance releases

Under this model, initial certification requirements should be more stringent than for sustaining qualification. Certification requirements will be more stringent if changes add/impact government unique functionality or add significant new functionality of interest to the customer.

An additional consideration may be “quality” metrics to determine retest requirements. These can be viewed as a way of rewarding vendors for good performance. For example, in labs that perform testing for a fee, vendors would determine what products they test based on the associated cost of the test. If the lab rewards vendors that demonstrate a commitment to certification and customer satisfaction by offering different levels of testing, a vendor may consider certifying more equipment if the total cost remains the same.

Some metrics may include:

- Whether the product has been evaluated previously
- Vendor performance in previous product evaluation(s)

- Product (and technology) maturity
- Feature/functionality change since previous evaluation (hardware as well as software)
- Vendor commitment to the certification process
- Customer satisfaction

Many labs have the concept of mandatory requirements that must be met and optional requirements that vendors can be evaluated against as a means of providing competitive differentiation. A lab might offer different levels of testing for these requirements based on the metrics listed above. For this exercise we'll refer to these levels as:

- Bronze
- Silver
- Gold

For a vendor with a good rating, and essentially only a new software release, the lab may only require Bronze testing. This would represent a simple validation of software functionality and, as a result, represent the least cost to a vendor. If a vendor had had problems in the past, the lab may force a Silver or even a Gold level of testing, requiring more extensive evaluation of function, interoperability, reliability, and/or performance to gain confidence in the product. After one or more successful evaluations, the level of testing required for that vendor may be reduced as a reward for good performance. In every case, Gold-level testing would be required for a new product.

Lab Operations

Lab operations can be complex, and are often hindered by personnel issues and the actual test implementation. Attracting and retaining qualified talent is an ongoing issue, as test engineers with experience quickly move on to take advantage of higher-paying job opportunities. Training of the lower-skilled testers doesn't happen, which prevents the lab staff from taking advantage of the latest technologies available in their field. The area of training is perfectly situated for an industry partner, who could easily align with the labs and quickly foster a more knowledgeable and motivated workforce.

These personnel issues are exacerbated by government contracting that awards test support services to the lowest bidder. Logically, this rewards the bidder with the lowest employee compensation. Over time, the employees grow dissatisfied with the lack of upward mobility, and they move on. High turnover of test personnel negatively impacts everyone in the certification process. Test labs should establish metrics that provide insight to cost versus productivity as opposed to just looking at operational cost.

Most test organizations will acknowledge that a certain level of testing is required to ensure products are up to standard. Most organizations measure defects found in the field to determine the adequacy of a test program. Therefore, while attempts can be made to build quality into products during the design and development phases, a certain level of testing is still required.

The challenge becomes: How to reduce the cost of testing, while performing the required amount of testing? Test automation would effectively solve this dilemma. While automating testing can be time-consuming and expensive in the short term, it has the long-term potential to significantly reduce the time and cost of testing. It also has the potential to make testing more repeatable and more comprehensive. Test automation has become the norm for equipment vendors because of the repeatability of testing (and results) and the associated cost savings. It is time for test labs to explore automation for the same reasons.

Test labs could effectively leverage the best practices from the industry in the area of automation, and they could engage vendors who would be willing to assist in the process. In the end, everyone benefits. The test lab is able to perform more testing in the same (or less) amount of time. Testing is repeatable. The vendor knows ahead of time what testing will be performed. The test process is more efficient, resulting in a better test value. Customers have a choice of a variety of products from a variety of vendors, and customers get a product that does what they require.

Summary

To truly address the complex issues facing today's certifying labs, there need to be changes in policy, process, and day-to-day lab operations. Moderate adjustments across all of these functional areas will significantly strengthen and more deeply seed networks with certified products. The labs will function more smoothly, and their customer satisfaction rating will improve dramatically. Adoption of best practices across all certifying labs, both government and commercial, is critical to the success of today's certifying bodies. Using the proven tactics employed in successful commercial labs will expedite the successful policy changes for government agencies that have yet to embrace these necessary best practices.

Once these best practices are inherent in day-to-day lab operations, proper metrics need to be employed to correctly measure the success points in all the relevant areas. The proper metrics, as defined in this paper, will be critical in employing the correct benchmark of measurement to prevent counterproductive results. If the emphasis is properly placed on increasing efficiency without impacting customer satisfaction, test labs will operate more efficiently and more effectively across all functional areas, and the end customers, lab employees, and vendors will all benefit.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA

CXX-XXXXXX-XX 05/08