Certification Overview

Authors

Ed Agis
Senior Engineering Director for Compliance & Certification Initiatives
NGS

David McCall
Senior Director, Industrial Standards
NGS, ISD

Jeremy Rover
Senior Network Standards Engineer
NGS

Greg Schlechter
Director, Time Technologies
PEMC

Table of Contents

1. Why a Formal Certification Program? 1
2. From Base Specification to Formal Certification 2
Interoperability Events 2
Testbeds 3
Golden Units. 3
Conformance Test Tool 3
3. Role of a Certification Authority 5
4. Lab Testing 6
Self-Testing. 7
5. Use of Derivative Products in Certification 7
6. Making use of Modular Certification 7
7. What are "Good Engineering Practices" for Standards Certification? 9
8. Conclusions. 10
9. References. 10

Introduction

The goal of a Certification Program is to deliver confidence to end users that Certified Devices from different manufacturers will interoperate. Over decades many organizations have developed programs that reliably deliver that confidence in different technology standards via various common strategies and structures. In the past, most of these certification programs existed in isolation from one another. Individual devices might be certified by multiple organizations, but each technology and each certification was only loosely connected to the other certification programs. This is changing. Industrial Automation is a leading example of end user requirements being met via a combination of intimately connected technologies that rely on each other. Developing standards for these complex combinations and then certification programs that deliver confidence in interoperability requires new approaches that build on existing ones.

Before delving into the new approaches, it is necessary to have a clear understanding of current approaches to certification. This certification overview provides:

- The reasons certification programs are necessary and their goals
- A framework for understanding the different elements of a certification program
  - Why each element exists
  - How they relate to each other
  - Best practices for implementing each element
- The tradeoffs that must be considered when building a certification program and how they may change over time

A future paper will describe the challenges arising from increasingly complex interactions between technology standards and their certification programs and how the latter can adapt to address them successfully.

1. Why a Formal Certification Program?

Implementing a formal certification program requires human, financial, and physical resources as well as effort and support from companies and product teams implementing the technology. With this investment in mind, it is worth understanding why a formal open certification program is critical to a technology ecosystem.

There are two main reasons standards exist. One is to ensure a defined level of quality, safety, or security is achieved. Another is ensuring interoperability between components built by different entities. Some standards have elements of both.

Examples of Standards

Quality / Safety / Security: USDA Beef (Choice/ Prime); Car Crash Standards (NCAP in Europe; NHTSA in USA); CE in Europe; UL in USA

Interoperability: Screw Threads; Wi-Fi; HTML

Interoperability & Safety: Electrical Plugs & Sockets; Fire Hydrants

Most technology standards focus on interoperability, which is the focus of this certification overview.

If a standard is relatively simple (screw threads, for example), and failure to comply is relatively obvious (nut does not fit onto screw), then a formal certification program may not be necessary. If the number of implementers is low, just getting everyone together in the same place at the same time may suffice to ensure interoperability for even complex standards (e.g., military projects). However, when the standard is complex AND the number of implementers is high, a formal certification program becomes the most efficient way to ensure interoperability.

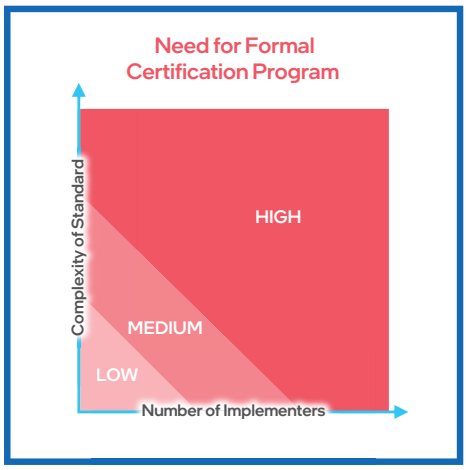

Figure 1. Relationship between the complexity of the standard, number of implementers of the standard, and the need for a formal certification program

The need for a formal certification program is particularly acute when end users want assurance that devices from different suppliers will interoperate, but they themselves cannot easily test every aspect of interoperability they may need. This assurance is the source of a key requirement for certification programs: they don't just ensure interoperability; they deliver confidence to end users that certified devices will interoperate. A short-term failure to deliver the former can result in a long-term problem delivering the latter, which greatly devalues the entire certification program. As a result, successful certification programs are designed to be highly reliable and protected against abuse.

2. From Base Specification to Formal Certification

Before developing formal certification, an organization must evaluate its goals, time-to-market, budget and other considerations to develop a certification strategy. Figure 2 sheds light on common certification strategies and corresponding time, effort, and cost (moving from left to right). The end goal in all cases is to ensure ecosystem interoperability.

The resulting certification strategy may include one or more of the following:

- Interoperability Events, attended by members of the standards organization
- Testbeds, hosted by the standards organization, their members, or Test Labs
- Golden Units, supplied by members of the standards organization
- Conformance Test Tool(s), often developed by the standards organization, validated by the relevant Certification Authority (see below), and hosted by labs (or, occasionally, validated for self-testing for certification)

Not all programs include all elements but, in general, programs start with Interop Events and add elements progressing from left to right. Each subsequent element requires more upfront investment but enables greater scalability.

Looking at each element in detail...

Interoperability Events

In the first step of developing a formal certification program from a base specification, interested manufacturers bring prototype equipment to events arranged by the standards organization, called Interop Events, IOP Events or "Plugfests." The participants work together to prove that the base specification, and their interpretations of it, can deliver interoperability. Agreement on a selection of features and configurations may be required.

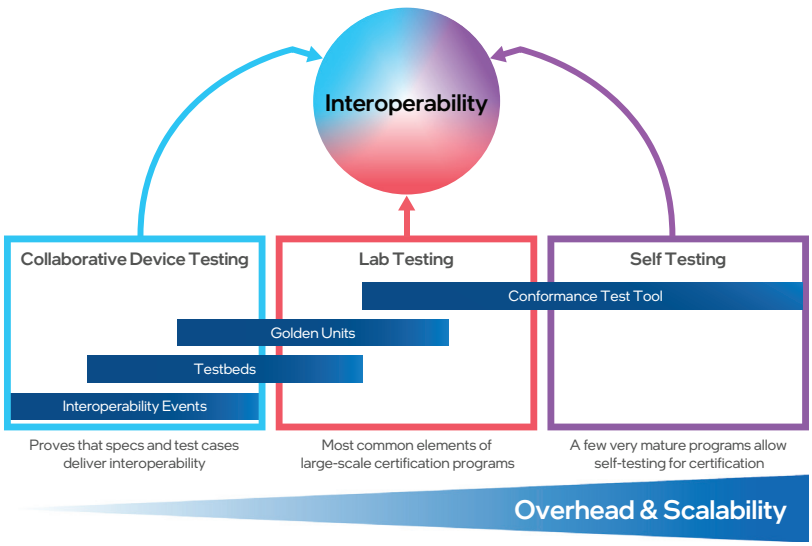

Figure 2. Overhead and Scalability of Common Certification Strategies

During the initial events, vendors aim to test every device with every other device in every possible scenario. This process, by definition, assures interoperability. Formal certification programs attempt to reduce the amount of testing required but still deliver very high confidence in interoperability.

As the certification program matures, interop events still take place, but their function evolves.

- As a conformance test tool is developed (see below), it will be included as part of the event to check that its test results correctly align with demonstrated interoperability.
- Participants will bring production equipment rather than prototypes to the events; it may even be a requirement during the initial months or years of certification that a certified device—or at least its manufacturer—has participated in an interop event.
- The focus of the events increasingly focuses on the addition of new features to the base specification and the test tooling versus testing older, mature features.

Interoperability events typically last anywhere from 1 to 5 days (2 or 3 days is most common) and occur between 1 to 4 times per year. They require considerable effort from both organizers and participants, including travel—often international—to the location of the event. The reward is a large quantity of data on how close base specifications are to being fit for purpose. The events also act as target points for participants to develop implementations of the base specification and can thus drive deployment. On the other hand, if they are the only way for companies to check their products are interoperable, waiting for the next event—especially if they are infrequent—can delay deployment. Successful standards will also reach a point where the logistics of running large events become unsustainable, which is where the elements below come in.

Testbeds

Interoperability events only permit testing for a few days every few months. Testbeds are designed so that manufacturers can test their equipment at any time, against an array of "known good" devices. They are especially useful when a standard is designed to enable large systems, i.e., typical deployments involve interoperability between not just two devices but between tens or hundreds of devices, with many different device roles.

Testbeds cover a range of formality. During the early stages of developing a standard, they may simply be a selection of donated devices that have performed well at interoperability events, kept at a single location by the standards organization, available for anyone to informally test against.

At the other end of the scale, there may be strict criteria for inclusion in a testbed (similar to golden units—see below), including multiple, identical testbeds that may be set up in different locations or that testing will be run according to a detailed test plan. In some cases, the testing may be run by a test lab, and successfully passing is a prerequisite for certification.

Between these two extremes are many variations. Examples include: testbeds hosted by university departments with some funding from the standards organization or their key members and testbeds hosted by individual companies aimed at proving the standard's ability to meet their specific requirements. In all cases, testbeds offer a more scalable solution than interoperability events through the simple expedient of being available all the time.

Golden Units

Many certification programs select "golden units" from commercial equipment and/or develop reference equipment from multiple vendors or open source. Golden units are "known-good" devices against which devices must demonstrate interoperability in order to be certified and are usually production devices. When testing a device against a golden unit, the tests are usually defined in detail in a Test Specification and are usually run manually—although some certification programs require inclusion of a dedicated test interface and/or test modes to initiate particular behavior. As the certification program matures, golden units may be hosted by a test lab and used as part of a pre-certification step before a device is submitted for certification. Not all standards employ golden units as part of certification, and for those that do employ them, the formality of the process varies widely. As the availability of golden units and the development of test tools mature, much of the manual interop testing starts to ramp down with conformance testing that fulfills similar requirements.

Conformance Test Tool

Most large-scale certification programs employ some form of conformance test tool (CTT) that is built to put a device through its paces as defined in the test specification. Test tool strategies (conformance) require selecting one or more test tool vendors, a validation process, and acceptance criteria for when to start certification. One big advantage of a CTT is its ability to run "negative" tests, e.g., how does a device respond to a malformed packet? Interoperability testing typically cannot check responses to "negative" behavior as production devices are not designed to behave in negative ways, e.g., produce malformed packets.

Usually, test labs carry out the required testing using the CTT and generate independent test reports for consumption by a standard's certification authority (see below).

Most certification programs also make the CTT available to members of the standards organization so they can test their device against the CTT prior to formal lab testing. Depending on the standard, the utility of the CTT may be limited by the need for specialized equipment or training. A few, very mature certification programs ensure the CTT is sufficiently comprehensive and easy to use that they allow members to self-test for certification, with no need to visit a Test Lab. Self-test certification is the pinnacle of scalability for a certification program, but it requires a lot of time and effort to achieve. In addition to being very confident that the testing is robust and reproducible even when those running the tests are not experts, additional measures must be taken to ensure that results are not falsified, which presents its own unique challenges.

Figure 3 illustrates what typically happens when a standards organization engages in developing and deploying the various elements of developing a certification program:

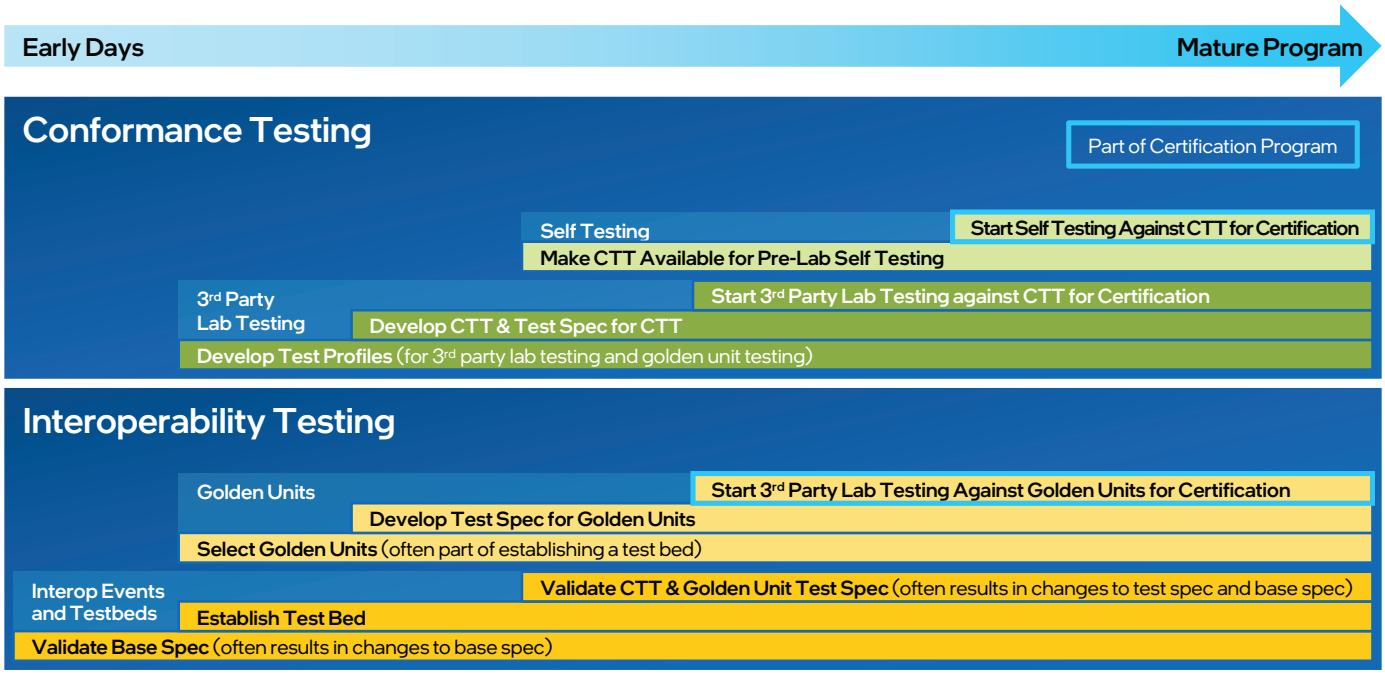

Figure 3. Generic Ecosystem Interoperability Program Timeline

Formal certification requires formalized testing, which is described in a test specification. This is not the same as the base specification.

- Base Specification—Defines what to do and how to do it.
- Test Specification—Defines what to test, how to test it, and the expected results.

Depending on the nature of the base specification, there may be additional steps before a test specification can be developed (e.g., feature and configuration selection for interoperability). These will be covered in a future paper.

The test specification defines the tests that are run, either manually or by the CTT, either with or without the inclusion of golden units. But there is a further challenge: how to ensure the tests are run consistently? Often tests will be run against devices on opposite sides of the world, months or years apart in time. These devices must still interoperate if they are brought together. It has been shown many times that simply testing against the same test specification is not enough. In the same way that there can be differences in interpretation of a base specification, different people may interpret and run tests differently, leading to inconsistent results.

If these inconsistencies lead to certified devices failing to interoperate, the certification program itself has failed.

This is the reason the final element of every modern, successful certification program exists: the certification authority (also called, in some organizations, the certification body) responsible for ensuring the integrity of the certification process. In terms of the elements already discussed, the certification authority:

- Selects golden units and test labs
- Validates that the CTT is fit for purpose
- Validates, often via audit, that the test labs are conducting tests correctly
- Checks test results from test labs (or, for some very mature certification programs, from self-testing) and determines whether a product should be certified as conformant
- Maintains a list of certified products

Figure 4 summarizes the relationship between the various aspects of a formal certification program.

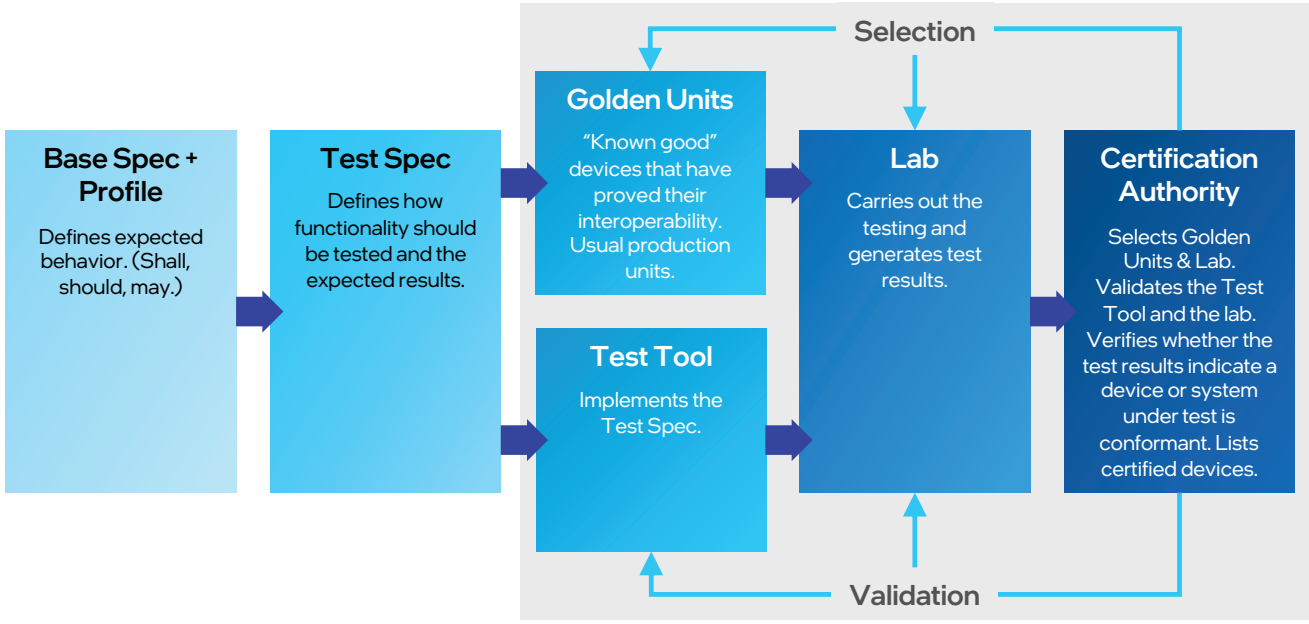

Figure 4: Aspects of a Formal Certification Program

More detail on the certification authority's roles, responsibilities, and structure is provided in section 3, below.

The requirements and benefits of enabling independent test labs are discussed in section 4, "Lab Testing." Section 4 also introduces considerations for enabling Self-Testing.

Within many certification programs, a clear distinction is drawn between a product that is "compliant" versus one that is "conformant." A compliant product was built according to a vendor's interpretation of the specification but has not passed testing by an approved standards certification process. The term conformant is reserved for products that have passed all tests for required mandatory functionality. The certification authority certifies conformant products.

A good certification program doesn't just deliver reliable interoperability, it does so efficiently. Part of that is covered by the elements already mentioned (golden units, CTT, self-testing) that avoid the need for every product to be tested for every feature against every other product. There are, however, two other important and common strategies deployed by many successful certification programs that deliver large increases in efficiency:

- Derivative Products. Where test requirements can be reduced or eliminated if a new product is sufficiently similar to an already certified product.
- Modular Certification. Where a subsystem can be certified separately from its inclusion in a product and products that include the subsystem—sufficiently unmodified—can similarly have their test requirements reduced or eliminated.

Derivative products, modular certification as well as best engineering practices for standards certification are all covered in more detail below.

In the development of a certification program, initially a lot of effort and overhead is needed to support a program. Over time, with the increase in maturity of a program, there is a migration of testing from interoperability testing to conformance testing and, ultimately, the potential of self-testing for certification.

The maturity also enables the certification program to reduce its complexity, i.e., moving from large interoperability testbeds filled with devices from multiple vendors to one or more test tools in the testbed along with the device under test. Along with reducing complexity for test labs, it enables developers to set up and easily maintain testbeds that better resemble certification testing.

3. Role of a Certification Authority

As previously mentioned, in some organizations the term "Certification Body" (CB), which is equivalent to Certification Authority (CA), is used; this certification overview uses the latter term. The certification authority is a member of a Certification Working Group (CWG) and authorized by the CWG to grant certificates for devices that have successfully passed all the required testing. In this role, the CA operates as a neutral body not staffed by member companies of the standards body. Conceptually, the CA sits between the CWG and the consortium's Authorized Test Labs (ATLs).

The roles of the certification authority include:

- Act as a neutral intermediary who can examine device information and communicate with an applicant while respecting confidentiality issues.
- Examine submitted applications, and determine whether they are ready to proceed to testing.
- Ensure that a conformance test tool has been validated and verified for use in the testbed.
- Assist with approving ATLs and overseeing and evaluating their capabilities and performance. The CA may revoke ATL status in cases of poor performance or misconduct (such as altering test results). The CA shall report any misconduct to applicable accreditation bodies such as ILAC (International Laboratory Accreditation Cooperation—http://ilac.org) and or IAF (International Accreditation Forum).
- Authorize the addition and removal of certified devices from the certified device registry.

- Evaluate initial appeals to negative testing outcomes, including waiver requests.
- Perform audits on certified devices.
- Participate in plugfest events in support of the development of certification tests for each new test specification release.
- Track the test result statistics and report them in an anonymized way to other relevant work groups and the CWG in order to identify test cases that need improvement and/or indicate unclear specification elements.

Of the roles managed by the CA, the Certification Registry is a public portal on the consortium's website that shows all the devices certified by the consortium. Information displayed on the certification registry includes:

- Name of the device
- Hardware and software version along with the date the device was certified
- Profile a device was certified to for conformance
- Vendor's contact for additional information
- Copy of the actual certification certificate

The information provided can be used by the end user, whether in B2B or B2C, to secure information on the device certified. For example, in a B2B environment, the end user may utilize this information to confirm a device meets the requirements necessary to operate in the end user's infrastructure. This requirement may be called out as a requirement when they issue a request for proposal on a project.

In a B2C scenario, the end user as a consumer may utilize the certification registry to verify that the device they are purchasing is certified. The number of consumers who actually take that step, however, is usually low; most rely on the presence of a certification logo. The logo is typically trademarked by the standard organization, and a license to use it in association with a product is only granted if the product is certified. This process provides a policing mechanism: if a company uses the logo with an uncertified product, the standards organization can sue them for trademark infringement, have the product removed from sale, and request damages.

4. Lab Testing

The primary goal of establishing test labs is to facilitate a consistent and predictable environment for certification. As you add multiple test labs to a program, establishment of the certification process and how the labs adhere to the process become critical in scaling a program.

Some minimum requirements for a lab include:

- Technical competence to perform tests defined in Test Plans and regular attendance at relevant standard body meetings based on their testing scope
- Identification and designation of a technology-specific Subject Matter Expert to be responsible for escalations as well as being the point of contact for all interactions with the standard body
- Having a dedicated lab space, equipment, and the required test tools
- Lab space that provides a "clean" environment for testing
  - In testing radio frequency (RF), an RF shielded room may be required
  - For networking applications, a dedicated test network separate from the control network may be required
- Ability to facilitate engineering and debug sessions with test engineers on lab equipment
- Measurement uncertainty calculations on record
- Quality Management System (i.e., log of all testing, calibrations, training, certification tests performed, etc.)

A certification program lists the test facility requirements in its policy or other documentation and will determine if a lab meets its requirements. Often this process is done through verification of industry requirements (e.g., "General requirements for the competence of testing and calibration laboratories," ISO 17025 accreditation), physical ownership of required test tools, training, membership in the standard organization, and routine audits.

Industry requirements in addition to the minimum requirements above are often verified in a lab audit. The auditing requirements are typically conducted by the standard body's certification authority and/or representatives from the certification work group. However, if required, an ISO audit is overseen by ILAC, which is an international organization for accreditation bodies. ILAC operates in accordance with ISO/IEC 17011 and is involved in the accreditation of conformity assessment bodies. ILAC scopes include the calibration laboratories (using ISO/IEC 17025), testing laboratories (using ISO/IEC 17025), and medical testing laboratories (using ISO 15189). Some standards bodies coordinate with ISO auditors to perform all auditing tasks required of a standards organization in addition to the ISO requirements in order to optimize the process.

Typically, a standards body sets criteria for the selection of labs. The standards body performs a selection across interested labs in order to maintain a competitive environment based on the demand for certification in the marketplace.

The selection criteria of test labs may consist of:

- Compliance with ISO specifications (e.g., ISO 17025, 65)
- Existing professional audits
- Geographical location
- Ability to scale testing support (i.e., multi-shift scaling)
- History of test and debug expertise
- Membership in the relevant standards body and standards participation
- Compliance with local government regulations
- Financial stability including insurance coverage and demonstrating that the lab is properly funded to run its operations

In addition to running test cases and providing access to test hardware, generally lab personnel are required to understand the technology being tested and to be able to provide assistance in debugging issues. The lab personnel are tasked with helping to determine the root cause of the issue: device under test, test setup, test tool, test case, or

an issue in the standard body's specification. Operation and deep understanding of the test tools and subject matter expertise become the true value-add for lab personnel supporting a certification program.

In general, third-party test labs are the default lab type required for certification programs. An independent "third party" provides all the features and capabilities above and imbues impartiality on certification processes in order to help avoid conflicts of interest.

Where a certification authority determines their process and tools can support a member company building a lab and performing certification testing, the authority may add supplier-run test facilities. These are often referred to as a "member company test labs." A member company test lab should support as many requirements test lab requirements that it can unless there is a business issue that makes support of a requirement difficult or impossible. One such example is requiring ISO 17025 accreditation of a supplier lab. This requirement forces a firewall between the engineering team and the test lab. In some cases, this requires a subsidiary be set up by the supplier company in order to meet the requirement as well as insurance requirements. One restriction that is common for first-party labs is to only allow them to test and certify products from their company. A member company test lab cannot provide certification collateral for an Original Equipment Manufacturer (OEM) company or other downstream partner. This is generally due to the insurance clause required of an independent test lab, where they have a legal responsibility attached to the accuracy of their test reports. The member company test lab would not certify others' products as they could not meet the requirement to stand behind their test results in a similar way.

Self-Testing

In addition to member company test labs, an organization may authorize self-testing for certification. There are a number of strategies that can enable self-testing including member company test lab authorizations. However, if a standards body is able to build trust into a test tool, they may be able to distribute or make this tool available to members to perform self-testing. Trusted tools often require tamper-proof executables and libraries, the ability to digitally sign test results, as well as a framework for providing secure updates to the tool.

The balance between building trust into a test tool and requiring member company test lab authorization also highlights the maturity of a program.

5. Use of Derivative Products in Certification

A derivative product differs from an original product in ways that are minor enough that the full set of certification tests is not required. The certification authority determines which sorts of changes can be classed in this way, and hence they are often referred to as "permitted changes." For example, when a product is submitted as a derivative, instead of running all the test cases multiple times, you would only execute the suite of test cases once or a defined subset of all test cases. Another example is the use of a derivative product that declares a reduced capability from the originally certified product (i.e., a subset of the originally tested features). In this case, the certification authority may approve a reduced set of testing to confirm that the product works properly, and the functionality supported has not changed. The vendor should declare whether the reduction of functionality dramatically affects the original product. Not all product architectures support the reduction of functionality without impacting other features. When this is the case, a new certification that tests all features should be submitted to the certification program.

The goal of testing for a derivative product is to demonstrate that the original product was not changed in a way that impacts its certified functionality. A vendor who reduces the supported set of functionality needs to perform good engineering practices and verify internally that the reduction did not impact the product (see section 7, "What are 'Good Engineering Practices' for Standards Certification?" for more details on this concept). A certification authority uses targeted test cases to verify functionality is unimpacted.

Any major software or hardware changes disqualify the original product certification from being used as part of a derived certification and require the full certification test suite to be executed; this includes major changes to the operating system for which an application is written.

A module differs from a derivative device. A module may not be a complete end product but may be designed to meet all the certification requirements and incorporated into an end product or reference design. A module in this instance may be certified using the full set of test cases and once certified does not get recertified unless a major change is made to the internal make-up of the module. The interface between the module and the end-product device needs to be well defined and requires integration and analysis that is out of scope of certification but should be employed as part of good engineering practice by device vendors or OEMs. If the module interface is defined by a Standards Developing Organization (SDO), a set of targeted tests may be used to verify a module without its integration into a reference device or product. When a certified module is integrated into the end product, the developer must note and provide evidence of the module previously being certified so additional testing of the module can be reduced.

6. Making Use of Modular Certification

Modular certification is appropriate when a subset of components that make up a certifiable end product is repeatedly reused in many end products in a manner that makes repeatedly running tests related to those components redundant. Instead, it is more efficient to identify and run a targeted set of tests on the subset of components so that it can be issued a modular certification. The ability to modularize a component comes down to the definition of the interface at the component's edge. If this interface is well defined in the standard, often simply testing the interface with a mechanism that emulates all functionality the component would be exposed to after integration is sufficient for modular certification. If the interface is not well defined or well tested, often the component is tested in a reference design as a part of a system. In this case, there are often system-level integration tests that must be run on subsequent products as the integration must be validated for certification. In the case of a well-defined interface, when a certifiable end product that incorporates the subset moves to certification, there is no need to repeat the tests that

were run on the subset of components. Instead, the end-product certification refers to the modular certification, and the manufacturer attests that no changes were made to the module. If the same subset of components is incorporated in 100 different certifiable end products, the tests on the subset of components do not need to be rerun.

In order for manufacturers to utilize modular testing, they are held to embodying “good engineering practices.” This concept is discussed in more detail in section 6, "What Are Good Engineering Practices for Standards Certification?".

Some good examples

- The Wi-Fi Alliance allows certification of Wi-Fi modules often, but not exclusively, in an M.2 hardware form factor and tested with production firmware and drivers in a representative system running the target operating system (e.g., Windows 10). The modular certification can then be applied to other systems running the same operating system that incorporate the same module, firmware, and drivers with only limited testing for factors that differ from the original system. For example, when a PC manufacturer (OEM) wishes to get a new laptop Wi-Fi certified, they may only need to do a few tests to prove that the antenna connection and placement haven't compromised RF performance.

  Note that the Wi-Fi Alliance makes extensive use of golden unit testing. There is no clear dividing line between the upper layers of the 802.11 software stack and the lower layers. When Wi-Fi was launched in 1997, there was no modular certification. Modular certification was added later when it was realized that a lot of testing was duplicating effort without adding value.
- The Bluetooth SIG has, from the start of its certification program, in 1998, supported modular certification. This was accomplished by establishing a clear dividing line between the silicon and lower layers of the Bluetooth protocol running in firmware (known as the Controller), and the upper protocol layers running on the Host device. This Host Controller Interface (HCI) is defined by the Bluetooth specification in extensive detail. The SIG tests Bluetooth modules (hardware and firmware) via the HCI. When the module is placed into an end device, only the aspects that might have changed—e.g., RF performance—are retested.

Based on lessons learned from the ProAV AVB certification, leadership companies in the ProAV market working under Avnu architected testing and certification that focused on the minimal testing needed for upper layer protocols for that market and what was needed to ensure these protocols were “using TSN” correctly without the need to retest all aspects of the underlying TSN mechanisms. The main benefit of modular certification is reduced costs for the ecosystem. While there is a higher overhead to establish modular certification, the reuse of the modules and the avoidance of rerunning what are often many of the most involved and expensive tests more than outweighs them. The enforcement of a clear dividing line between lower and upper protocol layers helps developers when resolving issues. Even including a minimum level of consistency between different implementations that include the same lower protocol layers makes it easier to compare ones that pass versus ones that fail conformance testing, thus easing debug problems.

Risks, complications and mitigations

- Incorporating the subset of components changes the behavior of the subset, invalidating the modular certification.
  - Only use modular certification for well-defined subsets with clear dividing lines and (if possible) interfaces to the rest of the end product.
    - If dividing lines are not present or available, the device will be tested as an end product and must pass all tests regardless of the component’s stated functionality (this is often called a reference design or white box implementation).
  - Where there is a risk, identify the characteristics that are most likely to be affected, and retest those to ensure behavior has not changed.
    - Example: retest RF signal strength to make sure antenna placement hasn’t compromised performance.
- Unintended consequences. When a component in a subset is updated (e.g., firmware), it may be judged to be minor and not require retesting for modular certification but then may subsequently change performance of the end product so that it would no longer pass certification. Worse: the subset is retested and passes, but the behavior of the end product still changes.
  - Be cautious when determining whether retesting is or is not required. Err on the side of caution because this is now one component in a system, which raises complexity.
  - Require periodic retesting to ensure that gradual updates of multiple software components have not, in aggregate, caused a system to fail conformance testing.
  - Make conformance test tools available to device manufacturers so they can run their own testing during development of software updates to ensure they don’t cause issues.
  - Mature certification helps. Clear delineation between the subset(s).
- Added complexity and overhead. Modular certification is not “free”; work must be done to develop the separate tests and processes.
  - Only apply when there are clear benefits, i.e., when there are many examples of the same subset of components being reused in many end products.
- Abuse of the system. When a certification authority makes it possible for some end-product manufacturers to avoid the cost involved in testing lower protocol layers by legitimately relying on prior modular certification of those layers, it also creates an incentive for others to reduce their costs by illegitimately claiming that same status. This risks the certification of end devices that are not interoperable and puts the ecosystem interoperability in jeopardy.
  - Good recordkeeping and a requirement to provide evidence that the subset of components for which modular certification is being claimed is sufficiently similar to the originally tested subset. Often this involves the provider of the subset to attest to its provenance.
  - Require spot testing of sensitive characteristics (similar to checking that a valid subset has been incorporated correctly—see above).

7. What are "Good Engineering Practices" for Standards Certification?

Many industries have coined the phrase "good engineering practice," but in general they relate to a set of procedures and documentation around manufacturer's product development. For example, in the telecom industry they utilize the R&TTE Directive 1999/5/EC, which refers to "good engineering practice" as well as compliance folders (i.e., documentation required by the conformity assessment procedures, see section 6 of Guide to R&TTE Directive 1999/5/EC) and relies on this directly where testing from an industry organization or other recognized body is unavailable. The manufacturer is required to test its own devices and hold itself to its own high engineering standard. A compliance folder is an element of this process and is the primary location for documenting these processes. The folder is also used to do differential and regression analysis on the product as changes are introduced.

The compliance folder and good engineering practices come into play especially when utilizing module certification, component certification, or anywhere integration of multiple components is required. Evaluating the impact of changes made during integration becomes the good engineering practice a certification authority is interested in. Depending on the maturity of manufacturers, a certifier may deem the industry capable of module certification and reuse of existing testing information. Generally when a manufacturer is trusted and authorized to do integration of a component or module without retesting or with a subset of the original testing required from a certification authority, they must always keep a record of their good engineering practices in a compliance folder that can be made available to a certification authority on request. As the information stored in this compliance folder is often proprietary and sensitive to the manufacturer, only authorized independent personnel may audit compliance folders. This would happen in the case of an interoperability issue or other test issue that the certification authority believes should have been caught in certification testing and/or the good engineering practices of a manufacturer.

A certification authority generally utilizes the compliance folder to bring transparency to the engineering practices of a manufacturer if there is an interoperability concern found in the field. These grievances are generally brought by other members to determine if there is a fault in certification, a standard, or the testing process and engineering practice of the manufacturer.

The following is an example of information a certification authority may include in its policy:

> *Any change to a Certified Implementation shall be assessed by the Supplier, who shall produce a documented evaluation of the impact of the change upon the device's functionality.*
>
> *If the Supplier considers that a change to the Certified Implementation has a significant risk of causing a change in the conformance of the device or of changing the results of any tests, then the Supplier SHALL re-test the device to ensure continued compliance with the requirements of the Certification Program. Records of all such testing MUST be kept by the Supplier in a Compliance Folder, along with the documented impact evaluation reports, and MUST be made available to the Certification Administrator on request.*

A compliance folder often contains the following information:

- Product identification—model name and number
- Kit number
- IEEE Standard base specification
- Certification profiles supported
- System Profile Release version
- Protocol Implementation Conformance Statements (PICS)
- Protocol Implementation eXtra Information for Testing (PIXIT)
- Test Case Category List Version (TCCL)
- Date of certification
- Certification certificates
- Declaration of Conformity & Mutual Non-Disclosure Agreement
- Certification Mark License Agreement
- Hardware identification
- Hardware change description
- Software identification
- Software change description
- Firmware identification
- Firmware change description
- RF module description
- RF module changes
- Vendor test reports and declarations
- Applicable waivers
- Change number, ID, and date
- Summary of changes
- Signed Letter from Original Certification Applicant granting permission to utilize the Original Certification in the Applicant's Derived Certification
- Signed Letter from Derived Certification Applicant attesting to changes made in Derived Platform

The folder brings light to the internal processes of the manufacturer. Good engineering practices generally involve following tenets and support these with documentation stored in a compliance folder:

- Strict requirement tracking, analysis, and definition
- Documented coding standards, code reviews
- Functional, continuous operation, and regression test plans
- Test results
- Quality criteria for Alpha/Beta/Final releases
- All certification-related information (as noted above)
- Multi-OS tests, regression as new versions are introduced
- Support plan, lifecycle, end-of-life target

8. Conclusions

Interoperable ecosystems of products are essential to advancing society—from a nut made by one manufacturer fitting onto a bolt made by a company on the other side of the world, to ensuring that your cellphone will connect to every one of the hundreds of millions of Wi-Fi hotspots around the world. Interoperability of enabling technologies reduces costs for everyone involved. It allows time and effort to be spent on truly innovative and differentiating features versus developing and maintaining a multitude of implementations that do essentially the same thing.

Ask people how technology companies and professionals deliver interoperable ecosystems, and most will refer to common specifications, usually developed by standards bodies, and stop there. While these base specifications are foundational, they are only one necessary element.

Numerous technologies and organizations have shown that a certification program for interoperability is essential, and that this involves several well-defined stages and techniques (e.g., base specifications, test profiles, test specifications, golden units, CTTs, test labs, certification authorities, etc.).

More complex ecosystems are now emerging that encompass multiple technologies from different standards bodies that must rely on each other, and each other's certification programs, for success. The end user's requirement is that the products they purchase interoperate.

As technologies and certification programs increased in complexity, the concepts of derivative certification and modular certification emerged as ways to minimize costs and reduce duplication of effort. The latter allows vendors who specialized in one layer of a complex technology to deliver a product certified for that layer of operation, on which vendors of other layers can rely, but both apply.

9. References

Some useful document resources, either cited in the paper or for readers seeking additional information, are provided here:

- ETS 400 306 - Methods for Testing and Specification (MTS); Protocol and profile conformance testing specifications; Standardization methodology
- https://www.etsi.org/deliver/etsi_i_ets/300400_300499/300406/01_60/ets_300406e01p.pdf
- ISO17025 - General requirements for the competence of testing and calibration laboratories
- https://www.freestandardsdownload.com/iso-iec-17025-2017.html

0321/AW/MIM/PDF Please recycle. 346145-001