

Difficulties in Providing Certification and Assurance for Software Defined Radios

John Giacomoni and Douglas C. Sicker
Department of Computer Science
University of Colorado at Boulder
Boulder, CO 80309-0430
{John.Giacomoni,Douglas.Sicker}@colorado.edu

Abstract— Certification and assurance processes have historically exhibited difficulties when there exists the potential for significant non-functional attributes. We define a non-functional attribute as a condition where the cause-effect behavior cannot readily be specified. Complex systems commonly exhibit such non-functional attributes due to the exceedingly large potential state space. In such systems, analysis based on formal methods becomes very difficult and emergent behaviors (or malicious behaviors that exploit non-functional attributes) can lead to a variety of unintended consequences - some benign and others harmful. Simply put, it is difficult to assure the behavior of a complex system. The shift towards highly flexible and adaptive software defined radios creates a potential complex system problem, and thereby exposes certain assurance and certification challenges for the present regulatory processes. We use certification experiences from the security community to motivate and highlight potential difficulties that may arise within the Software Defined Radio (SDR) space. We then recommend some steps that limit or account for these difficulties.

I. INTRODUCTION

Radios, to date, have had a long and successful history of certification¹ by the government spectrum authority and other organizations. These successes can be largely attributed to the static nature of these systems. We define a *static system* as a system where the functionality of its components are fairly predetermined and vary narrowly. The static nature of existing transmitters translates into mainly functional attributes, with minimal non-functional

attributes, and therefore present tractable evaluation² problems. Further, the inherent locality and physicality of transmitters permit “easy” containment of undesirable emergent behavior. Difficulties with certification begin to appear as we transition to smart software defined radios. Presently, smart radios such as cordless handsets, WiFi³, and cellphones are still tractable problems, albeit more challenging. The inherent fixed design and locality combined with client-server organization of simple cognitive radios keeps the problem bounded and therefore tractable. The problem becomes more challenging when the organizational constraint is relaxed and wireless devices begin to form ad-hoc⁴/mesh networks⁵. In these flexible operational modes, emergent behavior is most likely to manifest itself and malicious behavior is more likely to cause significant harm.

As we consider device certification, we should also consider the complexity of the spectrum models that might emerge. Broadly speaking, there are three primary spectrum candidate models presently being considered: The historical Command and Control model where the government spectrum authority has sole authority over spectrum and its use,

²We define *evaluation* as, “the process of assembling evidence that a system meets, or fails to meet, a prescribed assurance target.” [1]

³Devices compliant with the IEEE 802.11 standards.

⁴A form of self-configuring wireless networking in which connections are transient and formed in an ad-hoc as-needed basis.

⁵A form of self-healing networking in which routing continues in the face of broken nodes or connections.

¹We define *certification* as, “an authoritative attestation of conformity.”

a Property Rights model where spectrum is treated as property, and a Commons model where spectrum is held out as a shared public resource. In this paper we consider the differences between these models and variations, only as they intersect with different certification and assurance⁶ requirements.

One of the challenges when licensing or sub-licensing spectrum consists of determining the likelihood of damaging emergent or malicious behavior and how to control it. Various options exist including rigorous product evaluations designed to approximately prove correctness⁷, and financial penalties. The licensers may be in the best position to evaluate (potentially on an ongoing basis) how to balance their options. However, a device operating properly under one licensor may misbehave in a way that impacts adjacent spectrum (one the initial licensor may not have the incentive to address).

In this paper, we will briefly examine the history of functional, process, and security certification and their limitations. We relate our work to the recently released preliminary thoughts of the IEEE 1900.3 working group. We will examine the history of DRM⁸ as well as certifications as performed by the FCC for the public switched telephone network, digital television, and WiFi. Finally, we discuss the lessons that these prior certification efforts might shed on SDR.

II. DISCUSSION: IEEE 1900.3

Since submitting our extended abstract, the IEEE P1900.3⁹ working group has made available some preliminary information. [2] Since the group's stated scope is, "This recommended practice will provide technical guidelines for analyzing Software Defined Radio (SDR) software modules to ensure compliance with regulatory and operational requirements," [3] we felt it appropriate to briefly address the similarities and differences between our approaches at this time.

⁶We define *assurance* as, "our estimate of the likelihood that a system will not fail in some particular way." [1]

⁷Proving complete correctness of any real-world system is generally considered to be an intractable problem.

⁸Digital Rights Management

⁹Recommended Practices for Conformance Evaluation of Software Defined Radio (SDR) Software Modules

The working group describes the problem domain [4] in terms of device management by what we assume to be network operators, or spectrum license holders. They discuss issues involving the deployment and management of device software as well as third party applications. Four test categories of interest [4] are explicitly stated in the preliminary notes:

- **OTA Provisioning Testing** – *Verifies the ability of a device to correctly obtain & install applications over the air & to communicate problem with a provisioning server.*
- **Security Testing** – *Verifies sandbox boundaries and privileges of midlets plus verifies MIDP 2.0 security model.*
- **Performance Testing** – *Measures the time required for a device to perform operations or combinations of operations. (Ease of use factor)*
- **Stress Testing** – *Tests the behavior and robustness of the implementation when stretched to the limits of system resources. Ensures that device does not crash during continuous execution. (Reliability of use factor)*

These tests are all necessary prerequisites to the deployment of Command and Control networks similar to those of present day mobile phones. Any network which permits third party software modules to be loaded onto a proprietary device will need extensive security assurances coupled with reliable delivery mechanisms. At present, we feel it is rational to assume a rigid Command and Control structure to SDR spectrum models and hence certification and assurance requirements.

However, our focus is on exploring the full possibilities of SDRs including considering models in which consumers have direct access to the full expressive potential of the radios themselves. We are asking, what are the differing certification and assurance requirements for Command and Control, Commons, and Property Rights models? How do the requirements change if we prevent consumers from interacting with the SDR based network, permit only minimal interaction by exposing only a bit-stream interface, provide some level of cross-layer interaction [5], or expose the entire network?

To address these issues we must examine all four layers of an SDR system: the spectrum layer (interference models), the SDR networking layer, the device's operating system layer, and the applications layer. We believe all of these layers to be critical regulatory issues for the successful deployment of SDR.

III. DISCUSSION: CERTIFICATION

Certification is a common technique used to solve trust problems among parties where information asymmetries exist; it is often more efficient than relying simply on market factors such as reputation and warranties. Effective certifications are an external signaling mechanism denoting compliance with a known standard. The purpose of certification is to establish a certain level of assurance that a specific product conforms to its specifications.

Certification systems can be paid for either by the relying party or by the vendor. Examples of relying party certification include Underwriter Laboratories [6] and the US Government for the Trusted Computer System Evaluation Criteria. [7] The Common Criteria [8] reversed the TCSEC stance on relying party certification and instead pushed the fees onto the vendor. In these cases, care needs to be taken when instituting a regulated certification environment as perverse economic effects can occur including monopoly exclusion of new entrants, extraction of monopoly rents, and reduced quality of evaluations.

Broadly speaking, there are two core classes of certifications; those that certify products and those certifying processes. The goal of process certification is to cultivate a culture of excellence in a group, thereby ensuring the success of future projects. Product certifications fall into two sub-categories, those that can be specified in terms of functional attributes¹⁰ and those that attempt to evaluate a product against non-functional attributes.

In this section we examine the historical roots of certification, process certifications, and the need for specialized certification processes dealing specifically with non-functional attributes. Ultimately, we

¹⁰We define a *functional attribute* as, "a condition where a cause-effect behavior can be specified."

conclude that the certification techniques available today are not capable of providing a high-enough level of assurance to certify publicly available SDR products against a standards containing non-functional attributes.

A. Historical Roots

Certifications have been used throughout history as a means of marking the quality of a product. Recently, certifications have been used to signal alternative measures of quality such as safety and interoperability. We will only briefly sketch out this area as Sicker and Lookabaugh have already described the evolution of present day functional certification processes. [9]

The National Board of Fire Underwriters in 1901 incorporated Underwriters Laboratories as a non-profit organization to certify products as being safe. UL produced a list of approved products and demonstrated a correlation between certified products and reduced risk. Once the correlation became apparent in 1916, UL was transformed into a private entity creating a successful market for safety certifications. Similarly, in 1988 the cable operators formed CableLabs to solve interoperability problems. This organization provided a centralized testing facility to ensure products met their standards. Vendors wishing to sell products to or through the operators needed to supply a modest testing fee¹¹, accessible to most companies, and pass the compliance evaluation.

Traditional certification techniques generally rely on simple functional testing. For the domains of mass production, safety, and interoperability, these techniques are generally sufficient. However, functional testing techniques cannot ensure the quality of a future product nor can they solely provide a useful level of assurance for security requirements.

B. Process Certification

Process certification, unlike functional product certification, seeks to certify a company or a team's maturity or discipline and thus their ability to repeat past successes on future projects. In the case of manufacturing of reproductions, the correlation is

¹¹Fees range from 50,000-115,000 USD/product.

fairly intuitive. The challenge is in actually being able to repeat past performance on future projects. Both the ISO 9000 [10] series of certifications and the Capability Maturity Model [11] family of certifications attempt to ensure this.

The ISO 9000 series of certifications focuses primarily on ensuring that a company's organization and management structure are capable of maintaining a certain level of quality. Nations accredit certification bodies that in turn accredit audit firms. These audit firms are responsible for evaluating a company and its documented quality system, and ensuring the documentation matches the appropriate criteria and that the company is following the documentation. The certification is based on the notion that a good process can ensure good products, and that a good process evolves into an improved process. Unfortunately, some companies view the certification as a checklist item and once obtained fail to maintain the same level of performance. [1]

According to the Software Engineering Institute [12] "A Capability Maturity Model (CMM) is a reference model of mature practices in a specified discipline, used to improve and appraise a group's capability to perform that discipline." [13] The original CMM by the SEI was developed around the software engineering discipline, since then other CMMs have been developed for Systems Engineering, Systems Security Engineering, and others. [14]

The original Software CMM was organized into 5 maturity levels: Initial, Repeatable, Defined, Managed, and Optimizing. These levels represented a company's progress through different organizational capabilities with the overall maturity level being set at the lowest capability level. Recognizing certain inherent limitations in this staged model and to unify the family of CMMs, the SEI then began developing the Capability Maturity Model Integration. [15] In a nutshell, the CMMI accomplishes two key tasks: the unification of nomenclature and the addition of a continuous representation in addition to the staged representation. As part of the unifying process, the CMM maturity levels were redefined as: Initial, Managed, Defined, Quantitatively Managed, and Optimizing. The continuous representation allows an organization to grow across different

process areas in an independent fashion and is defined in terms of six different levels: Incomplete, Performed, Managed, Defined, Quantitatively Managed, and Optimizing.

Process certifications are a useful mechanism for evaluating a group's maturity level in designing products. Unfortunately, there may be a weak correlation between a group's certified level and its performance on future projects. The core issue is that existing process certification systems strive to ensure that a company or group is capable of continued success on the same core product, while information products are in constant evolution requiring constant evolution in the developers.

Taking a market perspective, organizations and groups have natural life cycles where they fight competitively to reach the top, then often stagnate. [1] In this manner, certifications may result in an inverse relationship with their desired outcome. The certifications imply trust, ensuring a supply of respected contracts with reduced competition. However once a steady stream of respected contracts manifests, pressures will mount to reduce quality in favor of short term increases in profit margins. This perverse effect can be attributed to the failure of certification schemes to include a revocation mechanism, preventing the market from Darwinianly selecting unfit companies for bankruptcy, acquisition, or improvement.

Further, these processes work best in large organizations where institutional knowledge can exist and survive the departure of a moderate number of individuals without threatening process maturity. In smaller companies and startups, the cost of formal software engineering methods are often viewed as inordinate and the loss of a key member can threaten any beginnings of institutional knowledge. Recently agile methods [16] have been gaining momentum among smaller institutions as well as larger organizations where requirements are constantly shifting to meet the needs of customers or the market as a whole. Considering many innovative and/or disruptive technologies are incubated in small companies, care must be taken before imposing any development processes.

C. Security Certification

Certifications for security requirements are intrinsically different from those covering functional or process requirements, as they evaluate non-functional attributes and model the user as malicious¹². When evaluating a system where users can be considered malicious, evaluations become significantly more complex. The reason, simply put, is that an evaluator needs to find every flaw while a malicious user only needs to find one. Further, one must consider the potential number of malicious users compared to the number of developers and evaluators.

Product evaluation is done by a combination of black-box¹³ and white-box¹⁴ testing and by comparing a product against its security target¹⁵. White-box testing is the preferred testing method for high levels of assurance, as one can attempt to mathematically prove the correctness of a section of code; the difficulty lies in correctly describing anything complicated. Black-box testing is also heavily used as products can diverge from their specifications, and it is required for the functional component of the evaluation. High levels of assurance require testing the complete system, hardware and software simultaneously, as a defect in one can lead to exploitations in the other. [1] Products deployed to consumers complicate matters further because there are often attacks against the underlying hardware that can be accomplished by skilled individuals with access to relatively inexpensive hardware. [1]

The initial formalized use of security certifications was the United States of America's Trusted

Computer System Evaluation Criteria. [7] The criteria were designed to enable the market to supply the systems the government wanted while obtaining the benefits of market competition. The government laid out the specifications in a collection of volumes known as the Rainbow Series [17], of which the Orange Book [7] specified trusted computer systems. The US Government certified and then paid testing facilities to evaluate products for compliance with specifications. Unfortunately, the desired secure systems market never developed due to the time and costs involved in developing high assurance products evaluated under the TCSEC criteria with the result that products were often a generation or more behind the current state of the art. [18]

Lack of flexibility and homogeneity led to the obsolescence of the existing security certification standards employed in America, Canada, and Europe and the creation of a unified scheme known as the Common Criteria¹⁶. [8] The overarching goal of the CC was to respond to the small markets, and hence small potential return on invested capital, and make trusted systems evaluation portable across national boundaries without the need for expensive redundant certifications. This was made possible by the creation of internationally recognized Protection Profiles and having the vendor certify against the market appropriate profile. Should there be no appropriate profile, the CC made it possible to "easily" create new profiles and certify against those while maintaining international acceptance. Further, Assurance Level was decoupled from protection profiles permitting vendors to make reduced Assurance Level claims about a product where they were not required without changing the functional or non-functional claims. The combination of the implementation independent Protection Profiles and Assurance Levels results in a Security Target against which one can evaluate a product. It is interesting to note the evolutionary parallels between the TCSEC/CC and the CMM/CMMI with the trend towards increased flexibility in how a product or organization is evaluated, at the cost of increased

¹²A *malicious user* is differentiated from other users in that they intelligently probe a system attempting to exploit vulnerabilities outside the specifications of normal use. Example: a routine takes a number from [1-10] as its argument, a malicious user would try parameters <1 and >10.

¹³We define *black-box testing* as, "a systematic form of testing utilizing only externally available information about the target of evaluation."

¹⁴We define *white-box testing* as, "a systematic form of testing utilizing complete information about the target of evaluation."

¹⁵A *security target* is defined as a product specific refinement of a protection profile. A protection profile is defined as, "a set of security requirements, their rationale, and an evaluation assurance level." [1] An *evaluation assurance level* is defined as the degree of rigor applied during the evaluation.

¹⁶CC v1.0 in January of 1996, CC v2.0 in May of 1998

complexity.

The CC introduced two critical changes in the certification process that have led to issues. Namely participating governments now certified international certification bodies and vendors were now responsible for certification fees¹⁷. These changes have begun to open the market of secure systems where the prior rigid and disjoint certification schemes struggled. However there is also one unfortunate side-effect, there is now a market for certifications where vendors seek the evaluators who will offer the path of least resistance. [1] Clearly this side-effect is not unsurprising; however, in an environment such as SDR we must be cautious and ensure that all evaluators are in fact equal, especially given the emphasis on SDR standards being international.

The process of certifying for security requirements poses numerous problems that must be dealt with prior to heterogeneous commercial use. The first problem is intrinsic in the evaluation process itself as increasing assurance is required “there are significant limitations on the practicability of meeting the requirements, partly due to substantial cost impact on the developer and evaluation activities, and also because anything other than the simplest of products is likely to be too complex to submit to state of the art techniques for formal analysis.” [19] This begs the question: how do we know when “we” are close enough? and who decides what the criteria are?

Assuming the costs involved in meeting high levels of assurance are met, the problem of authoring the PPs and derivative STs remains. In analyzing the LOCK/SMG projects, Smith notes that the “practicality [of formal assurance] hinges on the degree to which the formally modeled system properties represent all of a system’s essential properties.” [18] Therefore care must be taken to ensure each profile is written by representatives of all vested parties to prevent emerging markets from being closed off due to market incompatibilities with the specified PPs

¹⁷This change was borrowed from the European Information Technology Security Evaluation Criteria.

and STs, resulting in abnormal lock in effects¹⁸.

We feel it is also important to note that in some industries insurance models are being used to provide tolerable levels of assurance where the costs associated with increasing the certified assurance level of a system are not justifiable¹⁹. Restated, there are many situations in which complete assurance is not only infeasible but unnecessary as well.

The critical assumption of equality in evaluation skill also needs to be made; otherwise the certification bodies themselves can be gamed. [1] As discussed in the section on process certifications, companies exhibit natural life cycles and the quality of an evaluation can fluctuate potentially resulting in increased levels of risk due to incorrectly certified products being distributed to the public.

In domains where interoperability or personal safety are the primary concerns, the end users have strong incentives to exchange defective products. Security is an altogether different domain; consumers often find security technologies to be a burden and any product that can be used to alleviate the burden will be protected and therefore remain in circulation.

An important sidebar discussion concerns the difference in evaluation focus for SDR and traditional TCSEC. Traditional TCSEC systems are evaluated for their ability to preserve Confidentiality, Integrity, and Availability of the data and the system. In SDR we see an order reversal to evaluate in terms of Availability, Integrity, and Confidentiality. This distinction stresses the importance of the SDR networking layer over any transmitted information. This is particularly the case in SDR networks based on Dynamic Frequency Selection where spectrum is shared via cooperative protocols. Should any layer of the SDR device malfunction, the entire SDR network could be compromised due to direct and/or cascade failures.

¹⁸The more challenging problem is to ensure that future markets are not stifled by antiquated profiles. A complementary requirement should be to ensure that the ability remains to switch to future technologies without losing the benefits of past technology.

¹⁹See the Workshop on the Economics of Information Security for more information.

IV. DISCUSSION: DIGITAL RIGHTS MANAGEMENT

The shift towards information economies has made protecting a product increasingly critical and difficult²⁰. Physical products enjoy the protections of a constraining physical world where there are real costs associated with the production, reproduction, and distribution of products. To date, legal protections in the form of Patent and Copyright law have served to protect products when reproduction and distribution costs proved unable to curtail free riding on someone else's research and development. These legal protections hinge on the existence of legally visible entities acting as centralized facilitators. Information economies change the playing field by reducing the costs associated with reproduction and distribution to negligible levels as well as empowering individuals to become facilitators, resulting in inefficient legal protections.

In the remainder of this section we examine the threats posed to information products, attempts at mitigating them through technology, attempts at legislating these technological solutions, and the push for mandated technological solutions that can be trusted.

Digital information products are uniquely vulnerable to piracy since any copy can serve as a perfect master for unlimited additional copies. Old analog information products did not suffer from this systemic problem as any copy introduced noise and therefore information loss. This loss occurs not only in each generational copy, but in the original recording as the storage medium comes into contact with the input device. Information producers are becoming increasingly concerned as the market pressures them to release increasingly higher quality digital content to the general public without means of preserving existing market segments. Should a single copy of a digital product become illegitimately copyable, it becomes a simple exercise to distribute additional perfect reproductions of that 'original' copy via the increasingly high-speed net-

²⁰Inherent in this discussion is the assumption that it is in the economy's best interest to grant temporary monopolies to intellectual property to provide protection for the recovery of capital invested in the development of a product.

works to millions of users in an extremely short period.

A. Technology

Owners of digital information have been competing with those seeking to expand their use of information since digital information became a commodity. This battle can be viewed as an arms race where owners create new protection technologies only to have them repeatedly circumvented. Most protection systems involved checks introduced into a program that verify legal ownership by asking for a token²¹ from the user. The problem with these systems is that they can be circumvented either by reproducing the codes in a suitable form, or by altering the program itself to assert the existence of the token without the token being present. More advanced systems use external hardware to either decrypt selected portions of the code or to verify the integrity of the program itself. These more advanced systems require extra effort to circumvent, however eventually they tend to be circumvented. By design there must exist a complete and correct image of the information in memory that can be accessed and therefore altered by the owner of a computer. The same circumvention techniques can be applied to any modern protection technique used to protect information, provided users have full access to the memory of a system.

The overarching dilemma in DRM technologies is deciding how much protection is appropriate. As DRM systems have been repeatedly circumvented, content owners have increasingly migrated towards increased precaution resulting in increased perceived security at the expense of fair use. [20] We say perceived because as long as there were no legal consequences for creating technologies that exploited class-breaks²², these increasingly precautionary technologies served no purpose beyond the stimulation of large numbers of minds dedicated to

²¹We defined a *token* as, "a piece of information asserting certain rights." Examples of tokens include codes hidden on the physical distribution medium and codes stored in a manual.

²²We define a *class-break* as, "a vulnerability that once discovered is effortlessly reproduced for all existing systems with the same vulnerability."

preserving their definition of fair-use and enabling everyone else to do the same.

B. Legislation

The Digital Millennium Copyright Act [21] sought to address these issues by adding legal protections against circumventing, or producing circumventing technologies for copy protected technologies. Businesses could now deploy their information maintaining the ability to segment the market through product differentiation as no corporate entity could enter the market by offering tools to reformat or repackage their proprietary product, provided it was encapsulated in copy protection technology. These copy protection restrictions remain in place, and are protected by the DMCA, even if the protected information is not copyrightable²³. These protections are ineffective against numerous individuals and entities that are not legally visible. The Recording Industry Association of America has been maintaining a legal campaign against individual traders with uncertain effect.

In the recent past, various senators have proposed legislation designed to further protect the interests of copyright holders. Senator Fritz Hollings proposed the Consumer Broadband and Digital Television Promotion Act [22] (S.2048) designed to prevent the sale or distribution of products that did not include copy protection technologies set by the federal government. Senator Orin Hatch introduced the proposed Induce Act legislation whose purpose was to overturn the Sony Betamax case [23] because “A secondary-liability rule that punishes control and immunizes inducement is a public policy disaster.” [24] To date neither of these bills has passed in any form, although the FCC did add the Broadcast Flag [25] order to the regulations for digital television. Recently the US Court of Appeals invalidated, on the grounds of authority, the Broadcast Flag [26] order.

²³Many have argued the DMCA used in this fashion is a clear effort to abridge one’s ability to use the fair-use defense by ensuring a violation cannot occur.

C. Trusted Computing

Elements of the computer industry recognizing the difficulties of enacting and enforcing legal protections against independent and globally distributed entities are seeking a preemptive form of self-regulation by pushing trusted technologies²⁴. Microsoft and Intel have joined forces with other leading technology companies²⁵ and formed the Trusted Computing Group [28] whose mission is to develop trusted computing technologies as a platform for their DRM technologies. Specifically, the technologies being created by the TCG will prevent users from accessing protected information when it is stored temporarily in memory before being transmitted to an output device²⁶. The key is that only trusted programs will be permitted to access information protected with the trusted system, preventing the memory attack described earlier.

As discussed in the previous section, trusted technologies require that we have confidence, not certainty, in their ability to behave as expected. For this reason, there is a history in computing of evaluation and certification practices dating back to the 1970s and the Trusted Computer System Evaluation Criteria. [7] These practices attempt to quantify one’s confidence as an assurance rating and to make that assurance portable. It should be noted that there is a critical difference between the trusted computing systems developed for use by governments and those being developed by the TCG; TCG systems will be physically deployed into hostile environments²⁷.

²⁴We define *trusted technologies* as, “a technology that we believe will behave as expected.”

²⁵Membership at the time of writing includes AMD, Hewlett-Packard, IBM, Intel, Microsoft, Sony Corporation, and Sun Microsystems Inc. [27]

²⁶For the purposes of this discussion we are ignoring the analog-hole problem that permits individuals to capture an analog signal as it is transmitted to output devices and to recapture it as a digital signal. The vulnerability is that once a signal is converted to analog form it loses any digital protections it may have had.

²⁷A maxim of security is that hardware deployed into hostile environments is considered non-secureable and therefore compromised. [29]

V. DISCUSSION: FEDERAL COMMUNICATIONS COMMISSION

In this section we discuss the successful certification standards in the Public Switched Telephone Network, the issues involved in the Digital Television requirements, and the successes and flaws of the WiFi alliance standards. We also discuss the current SDR Certification Order.

A. *Public Switched Telephone Network [30]*

The PSTN provides an example of how the FCC successfully manages interoperability standards while it is not burdened by excessive centralized management responsibilities. The FCC accomplished this by having industry form its own standards-setting body, the Administrative Council for Terminal Attachments, under the auspices of the Telecommunications Industry Association and the Alliance for Telecommunications Industry Solutions. [31]

The FCC then pushed the certification work onto certified industry testing organizations. [32] Further, the FCC provided for future changes to the standards by reserving the right to revoke certifications from products that fail to comply with future standards regulating the PSTN. [33]

This system works, in general, because the standards are primarily functional standards. The functional attributes of the standard are designed to protect the PSTN by constraining devices to operate within specific parameters. The device has limited complexity and fairly fixed operational parameters. In the case of the PSTN, non-compliance has bounded potential damages limited to devices (or individuals) physically attached to the device. [34] Furthermore, there is little change possible in the operating parameters of the devices. This stands in stark contrast to the intended reconfigurable design of SDRs.

B. *Digital Television [35]*

In the case of digital television, the FCC is using a similar approach to the one currently used in the specifications for the PSTN by incorporating portions of the Advanced Television Systems Committee's [36] digital television standards [37].

Similar to the PSTN requirements the standard contains a mixture of functional and non-functional attributes. Televisions benefit from their nature as passive receivers and not broadcast devices, thereby limiting any potential physical damage from failure to comply with all the standards. This does not diminish the continued need for high-quality components such as receivers.

Televisions are intrinsically different from telephones in that they primarily handle information subject to protection under copyright law. The FCC, after multiple hearings decided to include protections for digital television broadcasts, the so-called Broadcast Flag [25]. This addition has come under attack by organizations such as the Electronic Frontier Foundation [38] and the federal courts, which said that the FCC overstepped its authority in requiring support for the Broadcast Flag. [39] Regardless, the question remains as to whether it is good policy to codify such standards by statutorily mandating them.

C. *Part 15*

The WiFi alliance provides a good example of the collaboration possible between the FCC and spectrum users, highlighting how industry collaboration can be effective. The example of the WiFi alliance also highlights how problems can arise when security technologies become codified. It is difficult to find fault with the WiFi alliance, as the technology is widely deployed by an increasing number of members. In creating a functional standard for collaborative use of the FCC's unlicensed spectrum they have demonstrated the value of self-regulation and they have proven that one can functionally certify to their standards.

Unfortunately, while the standard is functionally correct, there are numerous security problems in the standard's core design. The alliance has, at its own discretion, implemented several minor standard changes, attempting to address these security issues. These changes, however, were unable to address the core flaw in the design. The alliance, again at its discretion, has chosen to not force the issue by replacing the standard.

A different licensee might have chosen to push

significant standard changes to correct these flaws. The market obviously had an arresting effect on this change. Software defined radios would make updates of this nature as transparent as applying a software patch on your personal computer, thereby opening many new options for maintaining correct and efficient use of a licensee's spectrum in an efficient manner. Likewise, this ability to update and adapt opens a significant potential for increased non-functional attributes.

D. FCC Orders

Most radio transmitters in the US require FCC certification and similar requirements exist in other countries. The US certification process requires that a device be tested against a set of technical rules applicable to its intended operation. The results of these tests are filed with the FCC (along with an application and potentially some supplemental material). In some cases, these materials may alternatively be filed with a Telecommunications Certification Body (TCB). Changes to the operation of the device may require filing for a new certification; although certain changes may go through a streamlined process or not require re-filing under permissive change procedures. Testing typically covers field strength measures, frequency, output power and spurious emissions. Traditionally, this testing has been fairly straightforward, involving limited test cases.

In the most recent SDR Order, the FCC defines a software defined radio as "a radio that includes a transmitter in which the operating parameters of frequency range, modulation type or maximum output power (either radiated or conducted), or the circumstances under which the transmitter operates in accordance with Commission rules, can be altered by making a change in software without making any changes to hardware components that affect the radio frequency emissions." This evolved from an earlier definition that did not consider the "circumstances under which the transmitter operates." This additional phrase is critical to deal with the potential dynamic network protocol operation of an SDR. The FCC also required that the manufacturers implement security techniques to ensure that only

approved software can be loaded into the device and that users will not be able to alter operating frequencies, output power, modulation types or other radio frequency parameters in ways not approved. It is worth noting that the Commission gives flexibility to the manufacturers concerning the implementation of these security techniques. In this way the manufacturer is responsible for ensuring that the device will not be modified and if it is modified they will be expected to pull the device from the market and face the potential forfeiture and liability consequences. To ensure that these (and other) requirements are met, the Commission now requires that, in addition to the general certification process, applicants submit a "high level operational description or flow diagram of the software that controls the radio frequency operating parameters." This is a modification of earlier rules that required the applicant to submit a copy of the source code for the SDR. This signals the realization that reviewing source code will not necessarily provide the insight required by the certifiers and that reviewing the code would entail a huge effort. None the less, high assurance analysis often calls for formal methods and source code used in conjunction with white-box testing. The Commission adds that it retains its ability to request such source code or other materials if it should see this as necessary. Currently, the Commission is not authorizing the use of TCBs, but rather requiring that testing be done by the FCC labs. The details of the test procedures are fairly vague at this point. However, it is reasonable to expect test procedures to expand to address the adaptive nature SDR devices.

VI. FINDINGS

Recapping our findings from the discussion we reconsider the two primary techniques used to ensure a quality product: process and product certifications. Process certifications generally seek to ensure quality products that are on schedule and on budget by controlling the organizational aspects of a group. These techniques have been shown to be capable of permitting this level of control in certain groups. However, there are significant costs associated with this level of organization that present

a significant entry barrier to small groups that are working on defining and developing innovative products and disruptive technologies. For groups with a formal process model in place, exploring beyond the boundaries of their core competency may challenge their adaptive ability and hence the process model may provide no benefit or even act counter productively. Further, groups may exhibit natural life-cycles where their performance may lag in spite of a utilizing a formal development process model.

Product certifications are broken down into two key groups: those that evaluate products in terms of purely functional attributes and those which evaluate a products non-functional attributes as well. Schemes have been developed to handle products along the entire continuum. For products with non-functional attributes, certifications are assigned an Assurance Rating, as such systems exceed the limits of formal analysis and hence any evaluation scheme. Current schemes have shifted towards a flexible system where the functional and non-functional attributes are described in an assurance independent way, and then the evaluation assigns an appropriate Assurance Rating. A real challenge in such certifications is the authoring of the protection profiles as errors can have significant effects upon the market. Further, it must be noted that different groups may utilize the same profile, demand differing levels of assurance, and have different tolerances for errors in the profile itself. WiFi provides us with an example of the latter, where the way in which encryption was utilized in the Wired Equivalency Protocol was broken in the design, discovered post deployment, and tolerated without any significant arresting effect on its growth. Finally, it must be noted that different evaluators may have different abilities thereby resulting in certifications of varying quality, possibly to the point of opening up secondary markets for such certifications (forum shopping). Performing security certifications requires significant documentation, in terms of design, testing, and code reviews. Therefore, certifications involving products with non-functional attributes implicitly require the discipline of a formal process model. Similar to process certifications, product

certifications impose significant burdens upon small resource-poor groups.

The lessons learned from DRM are that even with strong motivations to technologically secure a system, the protections can still fail. As a result, legal pressures are applied to help provide incentives against breaking the protection technologies. However, often the desire for the content outweighs the legal counter-incentives and therefore fail. It is important to recognize the distinctions between individuals motivated to acquire content and those seeking access to spectrum.

While neither process or product certification scheme, alone, is capable of providing the assurances for products involving non-functional attributes, we believe there to be a space in which the costs and benefits can be appropriately managed by continued collaboration between government regulators and industry. Experiences with the evolution of security certifications showed that overly relying on assurance models can cripple the development and deployment of the products. A more rational approach is to balance assurance with the insurance that comes with assigning risk to the proper players. The question is how to best manage these difficulties.

Addressing the above issues we believe the following long term goals should be sought to ensure that SDR has the potential to reach its full maturity.

- Continued vigilance in protecting existing spectrum users; particularly spectrum for public safety
- Increasing self-determinancy within a license
- International cooperation on functional and non-functional attributes and certification for compliance.

The history of the FCC's regulations of Part 68²⁸ and Part 15²⁹ indicate a movement in these directions. Originally Part 68 had the FCC labs handling all certification in a white-box manner. As the telecommunications industry grew, the FCC labs were overburdened by the certification process and gradually switched to black-box testing and created

²⁸ 1975-present

²⁹ 1985-present

the Telecommunication Certification Bodies to handle the actual evaluations. Part 15 shows the FCC's willingness to experiment with a Commons model in which innovation within certain boundaries was encouraged, resulting in devices from remote garage door openers, to cordless telephone sets, to WiFi.

In the most recent SDR Order, the Commission stated, "We neither wish to have our process inadvertently be a barrier to the development and deployment of these technologies nor wish to permit the widespread deployment of radios easily susceptible of being misused to cause harmful interference to others." This balanced approach is echoed by the Order and serves as a logical starting point. However, as SDR devices continue to enter the market, it will likely be necessary to revisit a number of areas, the most obvious being: 1) the use of TCBs, 2) the adoption of protection profiles and 3) the development of SDR based test procedures.

VII. CONCLUSIONS

In this paper we have argued that there are significant difficulties in providing effective assurance and certification for products when significant non-functional attributes exist. We described how the difficulties involved in certifying smart software defined radio products pose significant problems in terms of how government may be involved within the certification process. Historically, industry and government has learned to effectively use a variety of certification schemes to ensure an efficient market. Therefore, it may be reasonable to expect to find an optimal balance between losses and benefits associated with differing certification schemes. The market, however, has not necessarily proven itself capable of addressing all public concerns. Therefore, we also believe that government should continue to play a role in defining emissions (and other SDR related) standards to minimize interference, and offer more flexible mechanisms for testing and certification.

REFERENCES

- [1] R. Anderson, *Security Engineering*. Wiley, 2001.
- [2] IEEE P1900.3. [Online]. Available: http://grouper.ieee.org/groups/emc/emc/ieee_emcs_-_sdcom/P1900-3/ieee_emcs_-_p1900-3.main.htm
- [3] IEEE. (2005, May) IEEE P1900.3 Project Authorization Form. [Online]. Available: http://grouper.ieee.org/groups/emc/emc/ieee_emcs_-_sdcom/P1900-3/
- [4] A. Kruetzfeldt. (2005, July) Recommended practice conformance eval SDR modules. [Online]. Available: http://grouper.ieee.org/groups/emc/emc/ieee_emcs_-_sdcom/P1900-3/
- [5] T. Weingart, D. Sicker, D. Grunwald, and M. Neufeld, "Adverbs and adjectives: An abstraction for software defined radio," in *Proceedings of the International Symposium on Advanced Radio Technologies*, March 2005, pp. 183–192.
- [6] "Underwriter's Laboratories." [Online]. Available: <http://www.ul.com/>
- [7] *Trusted Computer System Evaluation Criteria*, US Department of Defense Std., December 1985. [Online]. Available: <http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28.STD.html>
- [8] *Common Criteria*, National Institute of Standards and Technology Std. [Online]. Available: <http://csrc.nist.gov/cc/>
- [9] Sicker and Lookabaugh, "A model for emergency service of VoIP through certification and labeling," in *TPRC*, 2004.
- [10] *ISO 9000*, International Standards Organization Std. [Online]. Available: <http://www.iso.org/iso/en/iso9000-14000/iso9000/iso9000index.html>
- [11] "Capability Maturity Model." [Online]. Available: <http://www.sei.cmu.edu/cmm>
- [12] "Carnegie Mellon: Software Engineering Institute." [Online]. Available: <http://www.sei.cmu.edu>
- [13] "CMMI overview presentation." [Online]. Available: <http://www.sei.cmu.edu/cmmi/adoption/pdf/cmmi-overview05.pdf>
- [14] "CMMI models." [Online]. Available: <http://www.sei.cmu.edu/cmmi/models/models.html>
- [15] "Capability Maturity Model Integration." [Online]. Available: <http://www.sei.cmu.edu/cmmi/>
- [16] "AgileAlliance." [Online]. Available: <http://www.agilealliance.org>
- [17] *Rainbow Series*, US Department of Defense Std. [Online]. Available: <http://www.radium.ncsc.mil/tpep/library/rainbow>
- [18] R. E. Smith, "Cost profile of a highly assured, secure operating system," *ACM Trans. Inf. Syst. Secur.*, vol. 4, no. 1, pp. 72–101, 2001.
- [19] *Common Criteria User's Guide*. [Online]. Available: http://niap.nist.gov/cc-scheme/cc_docs/cc_users_guide.pdf
- [20] "Limitations on exclusive rights: Fair use," 17 U.S.C. 107.
- [21] "Digital Millennium Copyright Act." [Online]. Available: <http://thomas.loc.gov/cgi-bin/query/z?c105:H.R.2281.ENR>
- [22] "Wired News: What hollings' bill would do." [Online]. Available: <http://www.wired.com/news/politics/0,1283,51275,00.html>
- [23] "Sony Corp. of America v. Universal City Studios, Inc." 464 U.S. 417, 1984.
- [24] "Statement of Senator Orrin G. Hatch; Before the United States Senate on Introduction of the 'Inducing Infringement of Copyrights Act of 2004'," S.2560, June 2004.
- [25] "Redistribution control of digital television broadcasts," 47 C.F.R. pt. 73.9001, Federal Communications Commission.

- [26] *American Library Association, et al. v. Federal Communications Commission*, No. 04-1037 (DC Cir. App. May 6, 2005).
- [27] "Trusted Computing Group: Members." [Online]. Available: <https://trustedcomputinggroup.org/about/members/members>
- [28] "Trusted Computing Group." [Online]. Available: <https://trustedcomputinggroup.org>
- [29] *Guidelines for Writing Trusted Facility Manuals*, US Department of Defense Std., October 1992. [Online]. Available: <http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-016.pdf>
- [30] "Connection of terminal equipment to the telephone network," 47 C.F.R. pt. 68, Federal Communications Commission.
- [31] "Sponsor of the administrative council for terminal attachments," 47 C.F.R. pt. 68.602, Federal Communications Commission.
- [32] "Terminal equipment approval requirement," 47 C.F.R. pt. 68.102, Federal Communications Commission.
- [33] "Revocation of supplier's declaration of conformity," 47 C.F.R. pt. 68.350, Federal Communications Commission.
- [34] "Incidence of harm," 47 C.F.R. pt. 68.108, Federal Communications Commission.
- [35] "Radio broadcast services," 47 C.F.R. pt. 73, Federal Communications Commission.
- [36] "Advanced Television Systems Committee." [Online]. Available: <http://www.atsc.org/>
- [37] "Incorporation by reference," 47 C.F.R. pt. 73.8000, Federal Communications Commission.
- [38] "EFF: Broadcast flag archive." [Online]. Available: <http://www.eff.org/IP/Video/HDTV/?f=broadcastflag.html>
- [39] "USA Today: U.S. appeals court debates anti-piracy tv technology." [Online]. Available: http://www.usatoday.com/news/washington/2005-02-22-tv-piracy_x.htm