A REGULATORY FRAMEWORK USING AUTOMATIC CERTIFICATION SYSTEM FOR SOFTWARE DEFINED RADIO

Kazuyuki OKUIKE, Kenta UMEBAYASHI, Ryuji KOHNO (Yokohama National University, Yokohama, Kanagawa, Japan; kuike[ume, kohno]@kohnolab.dnj.ynu.ac.jp);

ABSTRACT

Under current radio regulations, it is illegal to change the configuration of a radio after its type approval has been acquired. However, the reconfigurability of a Software Defined Radio (SDR) terminal which is the benefits is possible by changing its software in the field. This contradicts the type approval under current radio regulations. Therefore, a new authorization procedure is necessary for system reconfiguration using SDR. A new authorization procedure requires techniques to prevent the operation out of the allowed limits of SDR in the field. In this paper, we propose a novel mechanism, called Automatic Certification System (ACS), as a solution to these regulatory issues for SDR. ACS is a system which gives type approval automatically to the software which affects the output power, central frequency, frequency band, modulation type and others in an SDR terminal. We also propose the ACS based framework which aims to distribute the burden of the software manufacturer, hardware manufacturer, and governmental authority. After that, we describe the inspection method and discuss about the case of a modulation module which can be Phase Shift Keying (PSK) and Minimum Shift Keying (MSK) schemes. Our simulations confirmed that ACS is able to certify the modulation software at the terminal.

1. INTRODUCTION

Recently, Software Defined Radio (SDR) has been recognized as an important technology for wireless communications, and the realization of SDR is now a reality [1-2]. There are now important issues about the standardization, security and type approval of SDR [3-7]. As an example, in a conventional radio under current radio regulations, it is illegal to change the configuration of a radio after its type approval has been acquired. However, the reconfigurability which is one of the benefits of SDR is possible by changing its software in the field. This contradicts the type approval under current radio regulations. The current radio regulations are designed to maintain the fairness and efficient use of electromagnetic radio frequency. A new authorization procedure is necessary for system reconfiguration using SDR. This paper focuses on a new authorization procedure needed for the type approval of SDR.

Techniques are required to prevent the operation out of the allowed limits of SDR in the field. This is considered in the following two approaches. Firstly, only the combination of software (SW) and hardware (HW) which has passed inspection can be used for reconfiguration. Secondly, SW and HW are inspected independently of each other. The first way prevents the operation out of the allowed limits of SDR completely, however, the number of inspections will increase greatly, and will be a problem for the governmental authority, HW and SW manufacturer. The second way decreases the number of inspections, however, questions arise about how the adjustment of HW and SW can be guaranteed. The Federal Communications Commission (FCC) in the United States has proposed a Class III Permissive change (C3PC) as the standard of type approval for SDR [3]. In this proposal, any changes in frequency, power, or modulation type of an SDR may be authorized as a C3PC. It requires that the applicant for a C3PC must submit test results, they should show that the equipment complies with the requirements for the services or rule parts under which the equipment will operate with the new software. Moreover, only the party holding the grant of the equipment authorization for the SDR is allowed to file for a C3PC. This procedure, however, requires software creators to apply for software authorization with the party holding the grant of the equipment authorization in order to approve the combinations of hardware and software. Otherwise, software creators must get the grant of the equipment authorization to certify the software authorization.

Since the development of software is dependent on the hardware making party, this proposal may prevent the development of software by third parties. Furthermore, if the number of software manufacturers increase, then the application using the C3PC scheme from the SW manufacturers to the HW manufacturer will also increase.
This will become a large burden on the HW manufacturer. Since the amount of application to a governmental authority

will increase enormously if the number of software and SDR terminals increases, it will also become a large burden for the governmental authority.

Recently, the Tokyo Institute Technology (TIT) proposed an Automatic Calibration Unit (ACU) to solve the problem [8-9]. The ACU always checks and calibrates data which passes from the software module to the hardware module in an SDR terminal. Using this proposed system, a governmental authority can approve the software and SDR terminal independently. This system solves the problems outlined previously in the C3PC, however, new problems occur. Since the ACU is always observing the signal, even while the correct software is mounted and operating correctly, the power consumption increases dramatically.

As a solution to this problem, we propose an Automatic Certification System (ACS) [10]. ACS is a system which gives type approval automatically to the software which affects: the output power, central frequency, frequency band, modulation type and others in an SDR terminal. It now becomes possible to give the approval to the software in a terminal, without applying to a governmental authority, by mounting ACS in the terminal. It becomes unnecessary to always observe the software, and the problems of power consumption are solved. Furthermore, it is possible to sharply decrease the number of HW and SW combinations to be inspected. We will show these things by investigating the framework of the type approval procedure of SDR using ACS. This framework is aimed for the software manufacturer to apply for the type approval independently from a hardware manufacturer. In this way, the burden of the software manufacturer, hardware manufacturer, and governmental authority is distributed. After that, we describe the inspection method of a modem module using ACS. First, the test signals and reference signals are prepared, then the test signals are put into the modulation module, next, the square error between the output signals and reference signals are calculated. It is judged whether the software is correct or not, using square error. This paper also examines if the inspection is conducted correctly.

This paper is organized as follows: In Section 2 the ACS is presented. Section 3 explains the ACS based framework. In Section 4, we show the inspection method of the modulation module using ACS. We conclude our paper in Section 5.

2. AUTOMATIC CERTIFICATION SYSTEM

2.1 The ACS Concept

The Automatic Certification System (ACS) certifies that reconfigurable hardware modules, which are defined by the SDR architectures, conform to the regulations. This is because an SDR is defined by software and the system is changed by software. The SDR, therefore, has to obtain

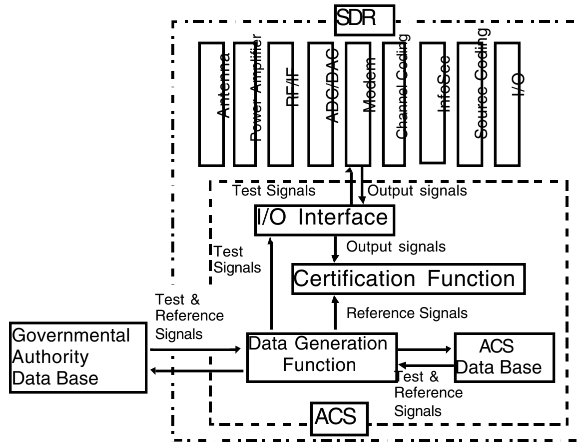

Fig.1 ACS Architecture

approval when the software is changed. The approval procedure using ACS differs from the conventional procedure. The ACS approves each reconfigurable hardware module, while the conventional procedure approves the complete device or system. So the ACS can approve, with a low load and in a short time, only the modules which are changed or updated. We can now realize to approval on board .

2.2 The ACS Architecture

The ACS is software for reconfigurable hardware, and therefore, can be changed or updated. Fig.1 shows the ACS architecture in the SDR terminal. ACS consists of an I/O Interface, Data Generation Function, Database, and a Certification Function.

The I/O Interface controls the test signals and output signals that are generated in the Data Generation Function for certification. It also sends the test signals to the reconfigurable hardware modules and receives the output signals from the reconfigurable hardware modules. After that, it sends the output signals to the Certification Function.

The Data Generation Function generates the test signals and reference signals for certification from the ACS database or the governmental authority database. Generally an ACS database can be used, but a governmental authority database is used if the new software downloaded is not stored in the ACS database. The ACS database and the governmental authority database contain test signals and reference signals for certification. The ACS database is included within the SDR systems (e.g., SDR terminal, SDR base station, and so on), therefore the ACS database is smaller than a database from a governmental authority. The database of such a governmental authority contains all test and reference signals. The Certification Function examines the changed modules using the output signals from the I/O Interface and test signals from the Data Generation Function.

2.3 The ACS Implementation

The ACS is made by the ACS creator which is the trust party such as Governmental Authority. Then, the ACS creator encrypts the ACS using a public key encryption technique. ACS is encrypted using the secret key of the ACS creator. Then, ACS is sent to the terminal and decrypted using the public key of ACS creator in the terminal. It is necessary to prevent tampering of ACS after decrypted in the terminal using some techniques. After that, ACS is implemented in the terminal.

2.4 The ACS Update

ACS can be update when ACS has some bugs, security holes or a new version is made. Tested signals and reference signals of ACS data base are updated when new software or modules are made.

2.5 Approval Procedure with ACS

There are 2 types of approval procedure, namely the fixed type and reconfigurable type. Fixed parts (e.g., Antenna Module, RF Module, Power Amplifier Module, and so on) are approved without ACS by the governmental authority using a spectrum analyzer or a network analyzer. Fixed parts can't be reconfigured, and therefore are approved only once. Reconfigurable parts (e.g., Modem Module, Info Sec Module, and so on) are approved using ACS when the parts are reconfigured..

3. REGULATORY FRAMEWORK USING ACS

3.1 Concept of the Regulatory Framework Using ACS

Before considering the regulatory framework of ACS, seven roles are defined.

(a) ACS Creator
The ACS Creator is the organization, which creates the ACS. Only one ACS Creator exists. As a concrete role, the ACS Creator performs creation of the ACS, maintenance, management, and creates the test pattern for software inspection.

(b) Governmental Authority
Governmental Authority is the certification authority specified by the government. Since the characteristics of a radio changes when the software in an SDR changes, the Governmental Authority inspects the characteristic of the portion which cannot be changed in the field, such as the RF module. ACS inspects the previous result to certify the software on board.

(c) Certification Authority
Certification Authority is an organization which gives infrastructures, such as Public Key Infrastructure (PKI) and Digital Signature (DS). It is not necessary to be a government authority, it can be an ordinary company.

(d) Operator
The Operator is an organization, which offers the infrastructure of Wireless communication.

(e) Hardware Manufacturer
The hardware manufacturer is an organization, which creates the hardware of the SDR terminal. The hardware manufacturer needs to apply the created hardware for type approval to the Governmental Authority. The Hardware Manufacture may sell the SDR terminal which has gained type approval as an SDR terminal.

(f) Software Manufacturer
The software manufacturer is an organization, which creates the software for an SDR terminal. Since type approval of software is given inside a terminal, it is not necessary to apply for it to Governmental Authority in advance. It is necessary only to use technology, such as PKI and DS, to identify the manufacturer of the software and to prevent illegal use.

(g) User
The Users is the SDR terminal user.

The regulatory framework for using ACS is now explained. First, the hardware manufacturer must gain the type approval of hardware from the manufacturer specified by the government, once the hardware for SDR is made. If type approval is given, the hardware manufacturer may create and sell the SDR. Next, a software manufacturer sells the software, after attaching its Digital Signature and other methods for verification of the software manufacturer. Then, the software manufacturer can sell the software to a user through an operator or a shop. A user can buy the SDR terminal, which type approval was given from a governmental Authority, and can use it. Moreover, a software manufacturer can be specified and only the software, which has not been altered, can be installed in an SDR terminal. ACS inspects the installed software at a user's SDR terminal before using it. If this inspection is passed, use of the software will be accepted. The ACS and data required for inspection can be downloaded and updated from the ACS Creator.

Table 1 Comparison of ACS- and C3PC- Based Framework

	Role?ACS?j	Role?C3PC)
ACS Creator	• Make ACS • Standardize ACS	• Not in Existence
Governmental Authority ?e.g. FCC, TCB, TELEC?j	• Authorization of SDR Terminal	• Authorization of SDR Terminal and Software
Certification Authority ?e.g.VeriSign?j	• Provide the Public Key Infrastructure (PKI) • Authenticate the identity of users (Digital Signature:DS)	• Provide the Public Key Infrastructure (PKI) • Authenticate the identity of users (Digital Signature:DS)
Operator ?e.g. NTT Docomo?j	• Provide the Wireless Communication Infrastructure	• Provide the Wireless Communication Infrastructure
Hardware Maker	• Make SDR Terminal and Acquire the Type Approval	• Make SDR Terminal and Acquire the Type Approval • Acquire the Type Approval of Software with Software Creator
Software Maker	• Make SDR software	• Make SDR Software and Acquire the Type Approval with Hardware Creator
User	• Use the SDR terminal without complicated operation	• Use the SDR terminal without complicated operation

3.2 Comparison with the C3PC Based Framework

Comparison of the ACS based framework and the C3PC based framework is shown in Table 1. In the C3PC based framework, when a hardware manufacturer develops the hardware for SDR, it has to gain the Type Approval of the combination of the hardware and all the software to be used in the hardware. Therefore, the load of inspection on a hardware manufacturer and the Governmental Authority increases. In contrast, in the ACS based Framework, the amount of inspection by the Governmental Authority will not increase markedly compared to the C3PC based framework. Moreover, when software is created in the C3PC based framework, a software manufacturer has to gain the Type Approval with the hardware manufacturer.
This is a big burden to the hardware manufacturer, the software manufacturer and Governmental Authority. Burden is not produced by the ACS based Framework in order to inspect software at a terminal, however, organization of the ACS is needed. Although a new role from the creation of an ACS is needed, the burden of a hardware manufacturer, a software manufacturer and Governmental Authority decreases and is distributed.

4. THE INSPECTION METHOD OF A MODULATION MODULE USING ACS

4.1 Simulation Model

In this section, the inspection method using ACS for the modulation module is considered, and a computer simulation is performed, the right software mounted in the modulation module can be: BPSK, QPSK, 8PSK, 16PSK, pi/4-QPSK, Offset QPSK (OQPSK), Minimum Shift Keying (MSK) and Gaussian-filtered MSK (GMSK) modulation schemes. The following two cases are considered as illegal software. One case is when the others modulation schemes are mounted when a modulation scheme should be mounted as shown in Fig. 2. The other case is when a part of the constellation moves to other part of the constellation, as shown in Fig. 3, and all cases of illegal software are shown in Table 2.

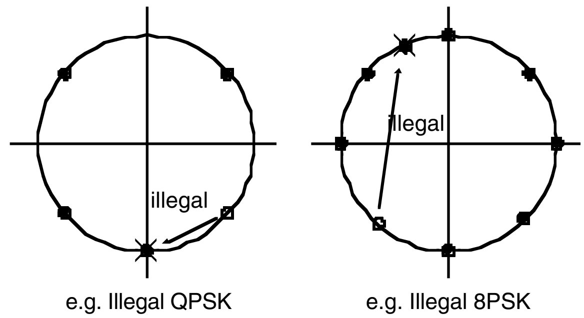

Fig.2 Example of Illegal Modulation Type1

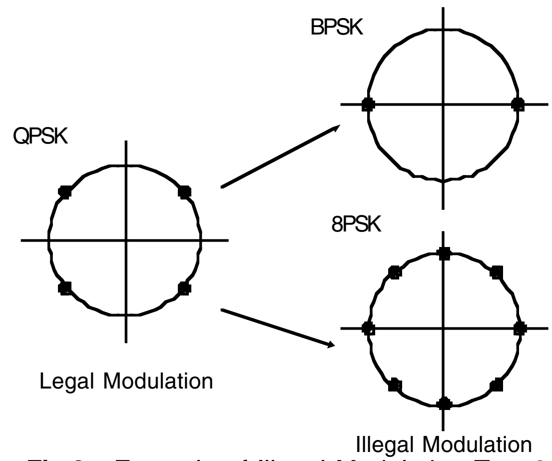

Fig.3 Example of Illegal Modulation Type2

4.2 Inspection Method

The inspection Method for the modulation module is described in the following procedures, and shown in Fig. 4. The ACS puts the test signals S_t into the modulation module. The modulation module processes the test signals S_t and returns the output signals S_{out} to the ACS, where f is the modulation function.

Table 2 ?@Error Pattern

	Correct Phase	Incorrect Phase
BPSK	$\theta_1 = n_1\pi$?@(n_1?@= 0,1)	$\theta_2 = \frac{n_2\pi}{8}$?@($n_2 = 0,1,\cdots 15$) *except*?@$\theta_1 \neq \theta_2$
QPSK	$\theta_1 = \frac{n_1\pi}{4}$?@($n_1 = 1,3,5,7$)	
Offset-QPSK	$\theta_1 = \frac{n_1\pi}{4}$?@($n_1 = 1,3,5,7$)	
ƒÎ/4-QPSK	$\theta_1 = \frac{n_1\pi}{4}$?@($n_1 = 0,1,\cdots 7$)	
8PSK	$\theta_1 = \frac{n_1\pi}{4}$?@($n_1 = 0,1,\cdots 7$)	
16PSK	$\theta_1 = \frac{n_1\pi}{8}$?@($n_1 = 0,1,\cdots 15$)	
MSK	$\theta_1 = \frac{n_1\pi}{2}$?@($n_1 = 0,1,2,3$)	
GMSK	$\theta_1 = \frac{n_1\pi}{2}$?@($n_1 = 0,1,2,3$)	

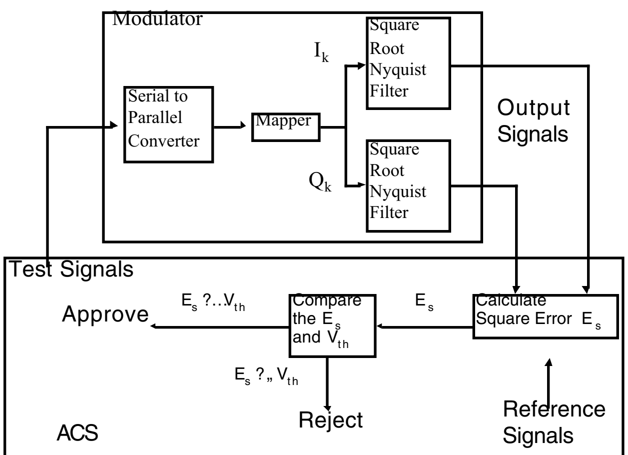

Fig.4 Inspection Method

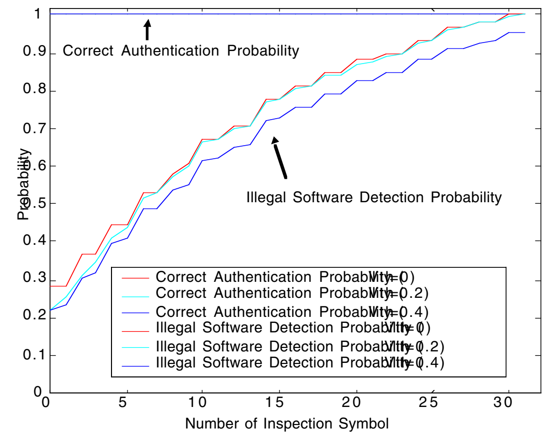

Fig. 5 Correct Authentication and Illegal Software Detection Probability without Error

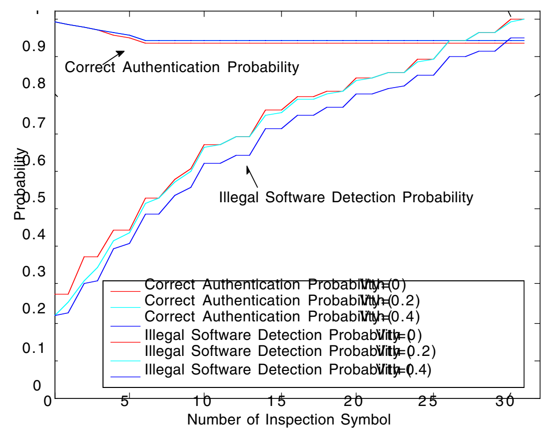

Fig. 6 Correct Authentication and Illegal Software Detection Probability with 1 Error

$$S_{out} = f(S_t) \qquad (1)$$

The ACS calculates the square error E_s between the output signals S_{out} and reference signals S_{ref}, where n is the number of inspected signals.

$$\sum_{t=1} \qquad (2)$$

After that, if the E_s (n) is smaller than a threshold value, the software will be approved, however, if E_s (n) is larger than a threshold value, it will not be approved.

$$E_s \leq V_{th} \rightarrow Approve$$
$$E_s > V_{th} \rightarrow Reject! \qquad (3)$$

4.3 Simulation Results

In this simulation, we evaluated the correct authentication probability and illegal software detection probability, changing the threshold value and the number of inspected signals with 0 or 1 errors, which don't have relation with illegal software, they are assumed just errors in digital system. Fig. 5 shows the correct authentication probability with no error. In this case, the correct authentication probability is always 1, therefore, ACS can authorize the correct modulation scheme perfectly. Fig. 5 also shows the illegal software detection probability with no error, this is high when the threshold value is small and the number of inspected signals are large, and tend to 1. Fig. 6 shows the correct authentication probability and the illegal software detection probabilities with 1 error. The Correct Authentication Probabilities are worse than ones with no error. These illegal software detection probabilities are similar to the ones with no error. Therefore, errors don't influence the illegal software detection. From the results of the simulations, correct authentication and illegal software detection probability with no error is the best at threshold value equal to 0. With 1 error, correct authentication probability is better when threshold value is larger, however, illegal software detection probability is better when threshold value is smaller. Tradeoff exists between correct authentication probability and illegal software detection probability.

5. CONCLUSION

In this paper, we proposed the concept and architecture of the ACS as a solution to the regulatory issues for SDR. ACS is a system which gives type approval automatically to the software which affects the output power, central frequency, frequency band, modulation type and other systems in an SDR terminal. We also proposed the ACS based framework, which aims to distribute the burden of the software manufacturer, hardware manufacturer, and governmental authority. After that, we described the inspection method in the case of a modulation scheme which can be PSK or MSK schemes. It is the best with no error that the threshold value is 0. With 1 errors, correct authentication probability is better when threshold value is larger, however, illegal software detection probability is better when threshold value is smaller. Using appropriate threshold value and inspecting some signals, ACS is able to certify the modulation software at the terminal.

6. REFERENCES

[1] J. Mitola, "The software radio architecture," *IEEE Commun. Mag.* , pp.26-38, May 1995.

[2] J. Mitola, "Software Radio Architecture: A Mathematical Perspective," *IEEE Journal on Selected Area in Communications,* Vol. 17, pp.514 - 538, April 1999.

[3] "Authorization and Use of Software Defined Radio: First Report and Order, " FCC. Washington, DC, Sept. 2001.

[4] "Report on Issues and Activity in the Area of Security for Software Defined Radio," Working Document SDRF-02-A-0003-V0.00, SDR Forum, Sept. 2002.

[5] Lachlan B. Michael, Miodrag J. Mihaljevic, Shinichiro Haruyama, Ryuji Kohno, "A Framework for Secure Download for Software-Defined Radio," IEEE Commun. Mag. , pp.88-96, July 2002.

[6] Klaus Moessner, Stephen Hope, Pete Cook, Walter Tuttlebee, and Rahim Tafazolli, "The RMA-A Framework for Reconfiguration of SDR Equipment," IEICE Trans. Commun., vol.E85-B, No.12, pp.2573-2580, Dec. 2002.

[7] Yasuo Suzuki, "Interoperability and Regulatory Issues around Software Defined Radio (SDR) Implementation," IEICE Trans. Commun., Vol.E85-B, No.12, pp.2564-2572, Dec.2002

[8] Munkhtur Togooch, Kei Sakaguchi, Jun-ichi Takada, Kiyomichi Araki, "Automatic Calibration Unit (ACU) and ACU employed Authorization Procedure (AMAP) for SDR," SDRF-02-I-0020-V0.00.

[9] Tien Dzung DOAN, Chih Fung LAM, Kei SAKAGUCHI, Jun-ichi TAKADA, Kiyomichi ARAKI, "DIGITAL PRE-DISTORTION LINEARIZER FOR A REALIZATION OF AUTOMATIC CALIBRATION UNIT," SDR Technical Conferece, pp.209-213, Nov. 2002.

[10] Kazuyuki OKUIKE, Hironori UCHIKAWA, Kentaro IKEMOTO, Kenta UMEBAYASHI, Ryuji KOHNO, "On-Board Automatic Certificating System (ACS) for Software Defined Radio," SDR Technical Conferece, pp.103-106, Nov. 2002.