A REGULATORY VIEW ON SECURITY REQUIREMENTS FOR RECONFIGURABLE RADIO

Jafar Faroughi-Esfahani (Motorola SPS, Aylesbury, United Kingdom; j.faroughi@motorola.com); Rainer Falk (Siemens, Germany; Rainer.Falk@siemens.com); Nigel Drew (Motorola SPS, Aylesbury, United Kingdom; Nigel.drew@motorola.com); Paul Bender (Regulierungsbehörde für Telekommunikation und Post, Germany, Paul.Bender@RegTP.de)

ABSTRACT

The next generation of the mobile communication systems will provide a massive range of services, with the means of software download and reconfigurability, providing increased opportunity to all involved parties (manufacturer, service provider, network operator, end user and application developers). Additional regulatory input will be required to gain maximum benefit and fairness, however not to the extent that the flexibility offered by reconfigurability is significantly compromised. In particular, if not anticipated and mitigated early, security issues will prevent development and deployment of reconfigurable radio systems. This paper describes some of the key security threats, and proposes some technical solutions – discussing how the current regulatory model might need to evolve to support the techniques. It also describes current regulatory thinking in Europe for SDR, and illustrates how the European research project IST-SCOUT provides a framework for collaboratively researching and evaluating solutions to the security and regulatory issues.

1. INTRODUCTION

Re-configurable Radio Systems and Networks will offer the next major leap forward in mobile and wireless communications, particularly in the light of the many existing world-wide air interface standards and the expected wide range of future broadband mobile and personal communication systems [1][2]. Clearly, reconfigurable terminals will offer greatly enhanced flexibility to the end user, supporting all types of radio systems (e.g. paging to cellular, numerous wireless LAN deployments, terrestrial to satellite, personal communications to broadcasting) as well as enabling the integration of many systems within the same platform. The performance and reliability of the reconfigurable terminal and the network is a common concern in the evolution of wireless communications from the perspective of users, network providers, manufacturers and service providers. Currently the regulatory bodies place requirements on radio equipment concerning:

- User safety
- Electromagnetic compatibility (EMC immunity)
- Radio spectrum use (EMC emission)

Conformance with these requirements has, depending on regulatory rules, either to be tested by an authorised regulatory body or testing house, or it can be declared by the manufacturer. In the EU, current approval of mobile terminals (mobile phones) is achieved by a declaration of conformity issued by the terminal manufacturer. In a reconfigurable system, however, it is not possible to test the equipment each time when new core radio software is dynamically introduced, or with each reconfiguration of the radio access technology. When radio software not provided or authorized by the manufacturer is installed, the manufacturer of the device can probably no longer be made responsible that the device meets conformance requirements. As a result there is need for an evolution of the regulatory approach to establish acceptable levels of safety, security, fairness of access to resources and integrity of the reconfigurable system. As well as the technology *placing* new demands on regulators, it is acknowledged by the regulatory community as a potential *opportunity*, offering an important mechanism to allow the modernization of spectrum engineering practices to improve spectrum efficiency.

Before reconfigurable radio is brought into the market, regulatory issues must be carefully considered and conclusions drawn for all market players [3]. This has begun with the publication of a Notice of Inquiry in spring 2000 by Federal Communication Commission (FCC) [4], the US regulatory authority. It has already published its First Report and Order on Authorization and Use of Software Defined Radios [5]. In Europe, the Radio Equipment and Telecommunications Terminal Equipment (R&TTE) Directive [6] was produced in April 2000 for this purpose. This paper reflects the regulatory aspects of SDR under the R&TTE Directive.

This paper focuses on system security and its potential impact on the evolution of regulatory practice. Through technical research in European Information Society Technology (IST) [7] projects TRUST[2] and SCOUT[8], section 2 describes specific threats raised by the introduction of reconfigurable radio, and poses some technical scenarios which could influence the regulatory approach. European regulatory perspectives on reconfigurable systems are discussed in section 3, and the

paper concludes by describing how the technical and regulatory perspectives will be addressed together through both European research and collaboration with the SDR Forum. The content of this paper is being investigated within the frame of European IST Project SCOUT (Smart user-Centric cOmmUnication environmenT).

2. ANTICIPATED NEW SECURITY REQUIREMENTS FOR RECONFIGURABLE RADIO SYSTEMS

Table 1 describes the key security threats associated with the reconfigurable radio system concept developed by IST-SCOUT [8]. The main issues are secure download of radio software, and protection of the reconfiguration process. It has to be ensured that only legitimate reconfigurations can take place that are in-line with the user and network preferences The reconfiguration signaling traffic has to be protected, and information used for the reconfiguration has to be reliable. Researching the means of mitigating against these threats has resulted in some potential new security requirements depicted in Figure 1.

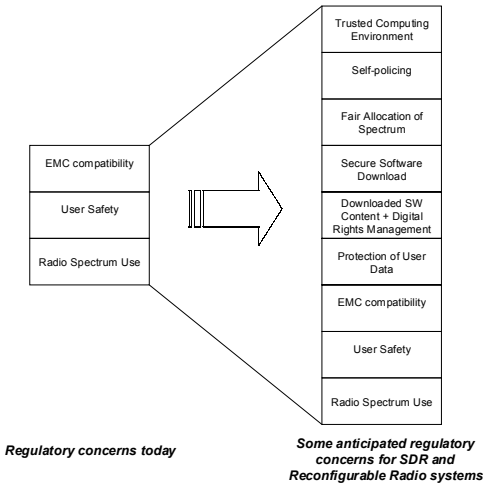

Figure 1: View of the current and the future (reconfigurable) communications regulatory rules

SCOUT provides a framework for early research within which these issues may be addressed collaboratively by technical and regulatory communities. This may result in proposals for extending the conformance criteria and evolving the role of the regulatory community to address the new scenarios introduced by reconfigurable radio. Figure 1 is by no means exhaustive: other regulatory concerns will emerge as the reconfigurable system is developed, and undoubtedly after deployment. However the beauty of SDR is its potential ability to reconfigure and hence the opportunity to improve its protection mechanisms as new threats and mitigation techniques are identified.

This section briefly describes the anticipated new security-related issues shown in Figure 1, which have arisen from technical considerations and which will drive the technical/regulatory collaboration in SCOUT. It will require further investigation to clarify which issues can be dealt with proprietarily, which ones need to be standardized by industry, and which issues have to be regulated. In general, a liberal approach seems attractive to allow future improvements and to achieve the highest benefit from the flexibility provided by SDR and reconfiguration.

SAFE RADIO PLATFORM:

It is anticipated that a number of features must exist in a reconfigurable mobile terminal to minimize the risk of intrusion, or corruption by malicious or buggy software which may lead to spurious radio emissions, degradation of service or even denial of service. For example:

- mechanisms to ensure boot code and core software is not corrupted or intercepted
- secure memory and resource management to ensure downloaded applications are isolated from core software
- secure storage for terminal identification codes (such as EMEI), encryption keys and security parameters
- non-reconfigurable and tamper-proof program code and supporting hardware to support self-policing and whistleblowing

By means of example, Figure 2 shows the "Secure Software Box" proposed in TRUST to support self-policing or whistleblowing detection techniques to mitigate against rogue terminal behavior and to support the application of corrective actions to eliminate the rogue behavior[9]. The software and supporting hardware of the "Secure Software Box" is non-reconfigurable. It may be controllable by parameters, which in turn must be securely protected by the trusted computing environment. The functions supervising a reconfigurable terminal can be placed both on the reconfigured terminal itself and in the network. The supervision can involve information gathered at several network nodes, that is merged and analyzed. Whether a reconfigurable device is allowed to activate a dynamically defined radio configuration might depend on whether the network that the device currently is using provides a service to supervise the radio emissions.

From a regulatory viewpoint, rather than approving all individual software and hardware configurations, which would seriously limit the scope of reconfigurability, it may be sufficient to check compliance with a minimum specification of the safeguards offered by the trusted computing environment, and perhaps classify the terminal in terms of any additional security features offered.

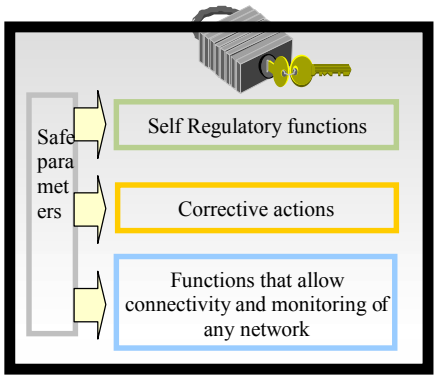

Figure 2: Secure software box

FAIR SPECTRUM ALLOCATION: In reconfigurable systems, functions that were formerly carried out solely in hardware, such as the generation of the transmitted radio signal and the tuning and detection of the received radio signal, are performed by software, perhaps controlling high-speed digital signal processors. The fact that these functions are carried out in software means that the radio can be programmed to transmit and receive over a wide range of frequencies and to emulate virtually any different desired transmission format. This permits SDR terminals to communicate using a number of different radio access technologies (RAT) and must comply with the RF emissions determined by the standard which defines that RAT. Failure to do so may result in degradation or denial of service to others. Therefore there is a need for regulatory rules to guarantee compliance with network standards for spectrum usage and power transmission. As a result a security method is required to control the transmission of the reconfigurable terminal to make sure it always transmits within the prescribed spectrum mask and at the right power [9].

Furthermore, in the longer term, the technology may permit the concept of spectrum-seeking cognitive radio. Here the wideband SDR device searches for spectrum availability, negotiates an appropriate service to support his application with both spectrum brokers and service providers, then modulates the allocated spectrum appropriately. A new regulatory approach may be required in this situation to ensure that the dynamic allocation of spectrum is administered fairly.

DOWNLOADED CONTENT PROTECTION: Downloading content, for example ring tones, games, music and streaming video is becoming more commonplace. Illegal copying or forwarding of these materials could bring massive losses of potential earnings to the owner of the material. It is essential to develop techniques for monitoring the usage, copying and forwarding of content and for the management of licenses permitting restricted access to content. Restrictions may include time of availability or buffer size, and specific hardware components with software management must be guaranteed to provide the appropriate protection as a complete system. But also the privacy issues of the end user have to be respected. Moreover the system may also be required to delete all traces of the content from the terminal upon expiry of a timed license.

SOFTWARE DOWNLOAD: Secure software download is a key technology for reconfiguration. Malicious software could invalidate properties required for type approval or assurance in a statement of conformance, and it could also lead to other types of harm. For example, it could circumvent other security mechanisms required for secure network access to a cellular network or a company's Intranet, or it could send a user's private data to unauthorized parties or make the device simply unusable. The effect of illegal alteration to radio software through error or by malicious intent could degrade or even prevent service within a cell: consequently there is a strong need for a robust and secure solution to verify the integrity and trustworthiness of downloaded radio software. A common approach is to use signed code where the provider signs a software package using a digital signature. Signed code allows the receiver to verify the provider and the integrity of the received software package independently from the download server the package has been loaded from. The reconfigured device verifies that the received code originates from a trusted provider and that it has not been manipulated. One approach is to re-use mechanisms developed for generic content download [10].

USER DATA PROTECTION: With the rapid increase in value-added services including e-commerce that require access to users' data, and the reliance on the part of the user for the device to securely store personal and valuable information, including currency tokens (the 'secure trusted device'), the privacy and protection of the users' private data become critical. Furthermore, in reconfiguration schemes which include network/terminal collaboration, user preferences or other user data may need to be stored in the network. The user data must also be protected from download of malicious applications, as well as being non-retrievable in case of theft or losing the terminal. For example it is possible to apply a method that deletes or corrupts the user's private data from the terminal whenever there is a breach of certain security criteria (this may require a means of retrieval within the system). Regulation authorities may need to consider stipulating that such a mechanism, meeting certain minimum protection criteria, is present in the terminal.

TYPE APPROVAL EVOLUTION: In the current mobile communication system, terminal equipment is guaranteed by the manufacturer (type approved), to

function within specification. But in reconfigurable systems, the functionality of User Equipment (UE) will change every time it reconfigures to a new Radio Access Technology (RAT) with the aid of software download. During this process there is a possibility for a UE to malfunction, saturate other users in the network, even disable the cell it is in and cause problems to the entire network. In order to control SDR mobile terminals, strict rules and conditions should apply in order to minimise software-induced problems to the network.

From the regulatory point of view it is important that reconfigurable equipment complies with the relevant technical specifications i.e. working frequency, output power, modulation technique, protocol etc in whichever mode it is able to operate. Given that this is no longer a practical proposition for all terminal software/hardware configurations, it is therefore essential to enforce deployment of methods and techniques within both the network and terminal, to detect and mitigate Rogue terminal behaviour. In this sense, the evolution of the type-approval process may involve 'boiling down' the critical system security threats into a minimal set of support features which all SDR terminals must provide (trusted computing environment elements, user data protection mechanism, appropriate DRM support, self-policing support, etc). The terminal may provide enhanced or additional mechanisms over those prescribed by industry standards or other conformance requirements, allowing access to additional content through enhanced DRM support or download of more critical core software upgrades. Such support may be handled through secure capability negotiation at download time, or alternatively through a classification of security support at industry standards or other conformance requirements. The latter solution is however less flexible as technologies develop.

Table 1: Security threats in a Reconfigurable Radio System

Security Threats	Description
Download and Execution of Malicious Software	Software download poses the threat that malicious software is downloaded that causes harm by accident or by intention. The software could simply not work properly or not implement the expected functionality and thereby pose a threat the reliability and availability, but it could as well implement malicious functionality as for example dialling premium rate numbers in the background, or any other of the threats described below.
Modification of Other Functionality	The purpose of a reconfiguration is to modify certain properties or functions of reconfigurable equipment. Other functionality not intended or authorized to be reconfigured could be affected by a reconfiguration.
Circumvention of Security Functions	Security functions, for example for secure network access to a cellular system or an Intranet or for m-commerce, have to be trustworthy themselves, but rely furthermore on secure storage of and protected access to cryptographic material and policy information. Unprotected reconfiguration could help to circumvent security functions not related to reconfiguration and thereby make them useless.
Easier Attacks	Reconfiguration could also make attacks against the wireless communication system easier and bring it in the range of a greater base of potential attackers. Attackers do not have to rely anymore on expensive equipment as signal generators or spectrum and protocol analysers, or have to build own special equipment involving e.g. reverse engineering and modification of proprietary, highly integrated devices. Instead they get easy access to open interfaces and could simply reconfigure off-the-shelf equipment according to their intentions.
Invalidation of Requirements on Radio Emission	Reconfiguration poses the threat that radio equipment may be brought into market where required properties as allowed frequency ranges and radiated power are violated during the operation of the equipment.
User Safety	Reconfiguration of radio equipment could, when the hardware allows, even endanger the health and safety of the user, for example when radiated power is too high.
Disregard of Preferences	Communication services could be used that do not match the preferences and expectations of the end user concerning available services, provided quality of service, and the involved cost. Also the preferences of service providers and network operators could be disregarded. As the intentions and preferences of users, different network operators and service providers could contradict, this point is not easy to solve. An example for possibly contradicting preferences is the selection of the radio access technology and network. While a user would probably prefer the cheapest technology that suits his service requirements, operators have an interest in the usage of the most profitable service and network and especially that a service and network offered by themselves and not by a competitor is used.
Disturbing Other Users or Systems	Reconfiguration could lead to emissions that harm other users and radio systems. Besides emitting in wrong frequency bands, using too high power, or wrong modulation schemes, also access to the radio medium could be modified in ways that have a negative impact on other users. As a single user or a small set of users could have an advantage in using

	"improved" configurations that implement unfair behaviour, this threat shows that the user cannot given full control over his reconfigurable equipment. This threat is obviously related to regulatory requirements, but its scope is broader than regulatory compliance as certain properties could be required by operators or non-regulatory standards who want to use their spectrum efficiently and provide good service to all customers.
Manipu-lated Reconfigur ation	The reconfiguration of terminal equipment will be supported by functions in the network, for example to assist mode monitoring or the mode switching decision. The reconfiguration process will be distributed between several entities in the fixed part and the mobile part of the communication system. Information used or even required for the reconfiguration or any other information exchanged between the involved nodes can be manipulated and therefore the reconfiguration process could be influenced in illegitimate ways..
Unreliable Operation	Unstable, non-working configuration. A configuration is activated that does not work at all or not properly. The consequence would be unsatisfied users, and high costs for customer care for the service provider. Unavailability of required reconfiguration services; software
Protection of Intellectual Property	Both hardware and software manufacturers have an intention to protect their development effort and to receive a fair compensation. Reconfiguration could make reverse engineering easier, and software could be used or copied illegally. When the user or the service provider can freely add desired features, differentiation of products by supported features will not work in the same way as for current equipment.
Illegitimate Access to Private Information	Sensitive information is required for the reconfiguration. Access to information about the preferences, used services, or the current location and configuration has to be controlled to protect the private sphere of a user. But also information related to a service provider or a network provider can be required to be kept confidential when the involved companies do not want to share data about their customers or network internals with competitors.

3. EUROPEAN REGULATORS PERSPECTIVE FOR THE RECONFIGURABLE SYSTEMS

Prior to the entry into force of the R&TTE Directive radio systems in Europe were subject to type approval. Type approval tests covered a set of parameters, including working frequency, output power and spurious emissions, and functionality tests for specific services (e.g. call set up and clearing, non-interference to the public network, etc.). Under the previous regime, equipment required new approval if any of these parameters were changed.

The R&TTE Directive has considerably simplified the procedure for manufacturers. In principle, manufacturers now need only declare the conformity of their products with the essential requirements of the Directive as applicable to the intended use in order to be able to place their products on the market.

This procedure is relatively unproblematic as far as equipment is concerned whose behaviour is determined by its hardware. Unlike today's equipment, the characteristics of SDR equipment (area of use, operating frequency, modulation technique, protocol, output power, etc.) can be modified during normal operation by a change in the software.

This means that SDR equipment would be able to load via software all the transmission standards in its feasible operating range, for instance 100 MHz-3 GHz. Likewise, a user would be able to use software to modify the equipment himself (by downloading software from the Internet) or even delete the equipment's functionality (pressing the reset button would delete the functionality and also eliminate any proof in the case of interference).

This functionality of SDR equipment raises various questions.

Who, for example, is responsible for conformity with the essential requirements and hence for issuing the declaration of conformity: the equipment manufacturer or the customer changing the software ?

Does the user have to issue a new declaration of conformity after a software change ?

If not, how is it possible to ensure compliance with the essential requirements by the equipment in its new mode ?

On the other hand, the possibility of modifying equipment characteristics by changing the software makes terminal equipment considerably more flexible, which can indeed also be of benefit.

In the following section we look in detail at the regulatory aspects of SDR under the R&TTE Directive. [11]

New Issues arising with SDR

Who is responsible for the declaration of conformity under the R&TTE Directive? The manufacturer? The user who changes the software?

Specific essential requirements – such as the definition of the intended working frequencies, output power and spurious emissions in other frequency bands – need to be fulfilled before radio equipment can be placed on the market and operated in a given frequency band. SDR equipment is designed such that it may be possible in the future to modify the operating parameters of equipment during operation by changing the software. Such a software change could conflict with the preconditions for placing the equipment on the market under the R&TTE Directive and for operating the equipment: the change

could cause the equipment to switch to a different mode (e.g. from GSM to TETRA, involving a change of frequency band, output power, etc.), for which no declaration of conformity with the essential requirements has been issued. The question then would be how to approach conformity assessment under the R&TTE Directive. It is unlikely that the user can be made responsible for compliance with the essential requirements because he cannot be expected to be familiar with all the legal aspects. If such highly flexible equipment is to be allowed onto the market, mechanisms are needed which ensure that the software available causes the hardware to operate only in those modes which are defined for the software and hardware in combination for the intended purpose and for which conformity with the essential requirements is ensured. This approach should apply at least to equipment using the radio spectrum, and is naturally dependent on various factors:

Which parts of the function of the terminal should be permitted to be modified through a software change?

The first question to be answered is which equipment functions the software should be allowed to change. Let us look, for example, at loading new games onto radio equipment. If the games had a defined area for storing the software which was not connected to the operating system and ruled out a change of operating mode, then such a software change would certainly not be critical in terms of compliance with the essential requirements under the R&TTE Directive. Other software changes which could be viewed as uncritical are, for instance, those involving input field or key functions and also the installation of new services not affecting the radio equipment's operating characteristics.

One possible way to ensure that the operating characteristics are not affected is to allow users to make updates using only software or public interfaces authorised by the equipment manufacturer. The radio equipment could, for instance, be designed to check that new software is signed by the manufacturer and to reject any unauthorised software. This should apply to all software changes which could directly affect the equipment's mode of operation. It therefore seems to make sense to have a separation between different software areas in the equipment, for instance areas that can be modified by the equipment manufacturer only. For example, the mode (DECT, GSM, IMT-2000) and frequency band could be selected by the network operator, the service provider could access specific services and interfaces, and application software supporting specific service offerings, like new games could be under the user's control.

Based on the essential requirements currently applicable, a declaration of conformity from the manufacturer could be adequate for conformity assessment under the R&TTE Directive and for placing the radio equipment on the market, on one condition: the manufacturer must be able to guarantee that the software areas designed for the network operator, service provider and user function independently of his area and cannot influence his operating system (DECT, GSM, IMT-2000, etc.).

What should be allowed to be changed without the users/owners permission?

In principle, we could say that no changes to the equipment software should be carried out without the user's/owner's permission. In practice, however, this could lead to difficulties because, for example, if it is a matter of improving the operating system software, the user/owner would probably not have enough technical understanding to assess the software changes. On the other hand, he should give his express agreement if, for example, a newly loaded service feature results in higher costs during use or if personal data are read out. Guaranteeing an appropriate duty of information, e.g. on the part of the manufacturer, network operator or service provider vis-à-vis the users/owners could be a task for the regulator.

Software download (security aspects)

The security aspects are one of the central points concerned with the introduction and use of SDR. How is it ensured that software can be downloaded and run only from interfaces intended for this purpose or that only software intended for the radio equipment can be downloaded and run? Would it make sense to agree on uniform standards for the relevant download interfaces? Should these interfaces and the authentication be prescribed in order to ensure that the SDR equipment can be used only with software in the assigned frequency ranges and that the radio equipment has a digital serial number to identify the manufacturer of the equipment and a signature on the software by the relevant providers (e.g. network operator, service provider, application software provider, etc.)?

Lets have a look on the requirements of Article 4.2 of the R&TTE Directive. This requires the public network operator to reveal its public interfaces and to describe them so precisely that a manufacturer can develop a piece of equipment for these interfaces and the services to be maintained over them. If no standardised interfaces are used for downloading software here in the SDR sphere, the effort to support the various interfaces with all their possible security requirements can be extremely high for the network operator and the manufacturer and thus unnecessarily expensive. It would also be sensible to have an instrument with which we could prevent unauthorised software changes that could have an impact on the correct operation of a radio terminal. Here, too, the question is posed as to how far the regulator should make proposals in this field.

Multiple uses of Frequency Bands by one Terminal

As an SDR terminal is easy to reprogram it would not be limited to being operated within a single fixed frequency range or only for a limited number of pre-programmed channels. It could be arranged so that it can work on every frequency that its design allows and it could be operated on channels of varying bandwidth with varying modulation formats. Furthermore, it should be possible to give the facilities some "intelligence" so that they monitor use by third parties in the spectrum and could transmit on free frequencies. These abilities could open up new possibilities in the field of frequency assignment and licensing. Instead of relying on a user finding a free frequency prior to transmission in a somewhat overloaded frequency range, a radio terminal could monitor a broad range of frequencies and find a free range with sufficient bandwidth in which the user can become active.

The use of SDR can also enable new types of joint frequency use not yet allowed by today's conventional equipment. If a mobile radio communications licensee has more frequencies than he directly needs, he could rent these frequencies to third parties at short notice. An SDR would facilitate such joint use. For example, a third party could acquire SDR terminals from a manufacturer that can be configured in such a way that different services can be offered in various frequency ranges. Once the frequency usage conditions have been negotiated the third part could rent a "package" comprising equipment and "transmission time" to end users who need communications capacity at short notice. He would load the software required to configure the equipment correctly when the end user enters into the rental contract. An alternative for the end user would be to contact the licensee directly with respect to the frequencies needed and then rent the correctly configured SDR terminals. The advantages for the public may be that there would be more communications capacity for the end user and that the spectrum could be better used as a resource.

In a slightly modified shared use scenario, the owner of a licence for a frequency block that is not being fully utilised could negotiate with a second party about approval for use of part of the spectrum at times when this part of the spectrum is available. The licensee could use an organisation channel to ensure that he primarily has access to the spectrum. In the case of a system of this kind, for example, the primary user of a signal would be transferred within the organisation channel as soon as the frequency range was available for use by the second user. The second user's transmitters would have to check whether the signal is constantly present in the organisation channel and they would have to cease use of the frequency block immediately when the signal disappears from the organisation channel. These checking/stopping capabilities in the SDR terminals would guarantee the primary user quick and reliable access to the spectrum when he needs it. There are therefore "no interruptions" in the jointly used spectrum. Frequencies that may not be constantly available are not suitable for some applications but they may be of interest for those applications where the user is prepared to accept a less reliable service for less money and for data applications for which there are alternative transmission possibilities. Functions such as those described in the paragraphs above could allow a more effective use of the spectrum. However, given the current legal framework in the EU, such a flexible use of the spectrum is scarcely possible for us in the Member States.

Signature of Software ? History Documentation ?

The software that may be used in an SDR could, for example, be signed by the manufacturer of the radio terminal and thus released by him for use in his radio terminal. This would guarantee that the radio terminal would meet the applicable technical requirements under all operating conditions. In order to ensure that software that has not been released cannot be downloaded, these radio terminals would have an authorisation system that checks the software for an authorisation code, which, for example, is added by the manufacturer, network operator or the national administration.

It may be necessary to specify methods that allow the user to note whether the desired operating software is currently loaded in an SDR terminal and that allow the market monitoring authorities of the Member States to check whether the software complies with the regulations in force. The question is whether such a procedure is needed, enforceable and practicable. What type of authentication system should be used ? Should it be a single system or should there be alternative systems ? Who should be responsible for generating the authentication code ? The manufacturer of the equipment or a different body ?

Do we need a method to show the information about the software loaded into an SDR ? If yes, what method should be used and what information should be shown ? It could make sense to have a history of all the software ever loaded onto the terminal, for example, so that subsequently, in the event of possible faults there would be the possibility of finding a cause. Otherwise, the person causing the fault could simply delete his software in his terminal and nothing could be proved.

On the other hand, one can argue that there may be definite parallels between an SDR and a PC connected to the Internet via a public network. What form does regulation take there at the moment ? The user can download any software from the internet. This software can change his entire operating system, open up new services to him without the regulator intervening. The user himself is responsible for no personal data being read out of his computer by, for example, installing a firewall

on his PC. If he uses his credit card to pay bills over the Internet, he does so at his own risk. Does this mean that no special regulations are needed for SDR ? The answer to this is not easy to determine.

CONCLUSION

The role of regulation in existing mobile communications is well bounded and defined, and is focused upon user safety, EMC immunity and emission, and system integrity. It is relatively straightforward to maintain general compliance through self-certification by manufacturers, given that behaviour of terminal equipment has to date been fixed by hardware and non-reconfigurable embedded firmware. The concepts of flexible spectrum access and software download offered by SDR technology and Reconfigurable Radio Systems pose significant security threats. Researching the means of mitigating against these threats indeed allows to determine how technology can be deployed in a way that minimizes the need for regulation. However, the sheer flexibility of the system concept potentially introduces significant new domains of concern, and it could be necessary to evolve today's regulatory model to constrain the reach of the problem without destroying the flexibility and the expected benefits of SDR and reconfigurability. The paper has discussed some of the potential threats, proposed some technical solutions to mitigate important threats and suggests how regulatory practices might be evolved to assist. When radio software is provided and authorized by the device manufacturer, the manufacturer can ensure compliance be assuring that only compliant radio software is activated. But when radio software originates from independent third parties, a possible approach could be that rather than checking compliance of all specific hardware/software combinations, which is very restrictive, alternative techniques such as self-policing of behaviour by terminals and networks, and 'whistleblowing' if rogue behaviour is detected by another terminal are be used. Such arguments result in a potential new model for ensuring compliance: rather than exhaustively checking behaviour, the terminal might implement a minimum set of features that ensure the essential requirements from regulatory perspective are met. Examples for such mechanisms are secure download of radio software, DRM support, self-policing, protection of critical or personal data, and safe execution within a safe radio platform. The challenge is to determine the exact specification of that minimum set of functionality necessary to ensure that essential regulatory requirements are met. Enhanced security support above the minimum set might allow additional flexibility, and might be negotiated at 'point of sale' through secure capability negotiation.

The paper has also described the current regulatory thinking in Europe illustrating just some of the key problems to be addressed. As well as highlighting the complexity of the problem, it has also discussed the opportunity offered by SDR technology to provide a means of achieving better usage of spectrum in the longer term through dynamic spectrum allocation, spectrum sharing and cognitive radio technology.

Each of these issues requires further research and a close cooperation between technical, regulatory, standardization and mobile communications business communities at both regional and global levels to assess feasibility. IST-SCOUT provides a funded framework to begin this cooperation, and to collaborate in the further development of technical and regulatory considerations discussed in this paper. Results sharing with SDR Forum provide the global perspective.

ACKNOWLEDGEMENT

This work has been performed in the framework of the IST project IST-2001-34091 SCOUT, which is partly funded by the European Union. The authors would like to acknowledge the contributions of their colleagues from Siemens AG, France Télécom – R&D, Centre Suisse d'Electronique et de Microtechnique S.A., King's College London, Motorola SA, Panasonic European Laboratories GmbH, Regulierungsbehörde für Telekommunikation und Post, Telefonica Investigacion Y Desarrollo S.A. Unipersonal, Toshiba Research Europe Ltd., TTI Norte S.L., University of Bristol, University of Southampton, University of Portsmouth, Siemens Mobile Communications S.p.A., 3G.com Technologies Ltd., Motorola Ltd., DoCoMo Communications Laboratories Europe GmbH.

REFERENCES

[1] "Reconfiguration of Future Mobile Terminals using Software Download"; IST mobile communications Summit 2000,
[2] IST-1999-12070 TRUST http://www.ist-TRUST.org,
[3] "SDR Equipment in Future Mobile Networks" http://www.ist-TRUST.org,
[4] "Federal Communication Commission" http://www.fcc.gov/,
[5] "FCC's FRO, ET Docket 00-47, December 8, 2001" http://ftp.fcc.gov/oet/dockets/et00-47/,
[6] "R&TTE Directive" http://europa.eu.int/comm/enterprise/rtte/,
[7] "Information Society Technology" http://www.cordis.lu/ist/
[8] IST-2001-34091 SCOUT http://www.ist-scout.org/
[9] "Locating and eliminating rogue software-reconfigurable terminals from network" IEE, 3G Mobile Communication Technologies, 2001 conference,
[10] "Open Mobile Alliance: Download Architecture, Version 1.0, Proposed Version 10-June-2002" http://www.openmobilealliance.org/documents.html
[11] "Reg-TP input to the SCOUT project" http://www.ist-scout.org/,