A SOLUTION FOR REGULATORY ISSUES WITH SDR

Nigel Jefferies [1], Walter H.W. Tuttlebee [2], Klaus Moessner [3]

[1] Vodafone Group R&D, The Courtyard, 2-4 London Road, Newbury, Berks, RG14 1JX, UK
Tel: +44 1635 67 3883, Fax: +44 1635 233440
nigel.jefferies@vodafone.com

[2] Mobile VCE, Grove House, Lutyens Close, Chineham Basingstoke, Hants., RG24 8AG, UK
Tel: +44 1256 31 6590, Fax: +44 1256 31 6589
walter.tuttlebee@mobilevce.com

[3] University of Surrey, Centre for Communication Systems Research, Guildford, Surrey, GU2 7XH, UK
Tel: +44 1483 68 3468, Fax: +44 1483 68 3468
k.moessner@eim.surrey.ac.uk

ABSTRACT

Software radio promises significant benefits for wireless telecoms systems, with enormous commercial potential. However, significant regulatory hurdles potentially exist which, if unaddressed, could delay or even preclude, commercial deployment of software reconfigurable terminals. If the characteristics of a handset's radio emissions can be changed by an end user, downloading unproven software from an unauthorised source, regulators may quite rightly demand stringent controls. The, here described, Reconfiguration Management Architecture - RMA – and its mechanisms provide a pragmatic technological solution to this issue. Developed within the framework of Mobile VCE research, the RMA offers an approach to the regulatory and security issues associated with terminal reconfigurability.

INTRODUCTION

Current regulation would not permit future users to change the radio characteristics of their SDR terminals, the RMA offers a detailed architectural framework that allows validation of a reconfigurable terminal prior to its authorisation for operation on a mobile network and provides with this the exploitation of the multiple flexible features as anticipated [1-4] for Software Radios. The main feature of the RMA is its platform independence, which facilitates the management and control of terminal reconfiguration processes. The RMA has been designed in a distributed manner, this ensures reconfiguration security and provides the possibility of preventing unwanted, undesired or non-standard compliant reconfigurations, whilst it still provides open programmability for third parties to develop and deliver the software implementation of radio modules,. This means that some of the architectural elements are located within the terminal (n.b. these are: a) the Radio Module Part (RMP) which executes the different instances of radio software and implements the actual radio and b) the Configuration Management Part (CMP), which manages the reconfiguration processes of the RMP), whilst a controlling element, to influence or even suspend terminal reconfiguration, is located within the network (i.e. the Configuration Control Part (CCP)).

The RMA also delivers the algorithms forming a reconfiguration process; this includes message sequences between the different architectural parts (i.e. CCP, CMP and RMP) but also mechanisms within the various modules of these distributed parts. I.e. internally, each part of the RMA consists of a number of different modules, of which each implements a defined set of tasks.

Beyond management and control, the RMA provides several possibilities where the regulator, network operator and user can influence, and if necessary stall or abort reconfiguration sequences, these are the 'Rules & Policies Tool' and the 'Virtual Configuration' as part of the 'configuration validation process' within a reconfiguration sequence. We describe the RMA details of the, its parts and mechanisms and show how the architecture facilitates that a regulator can delegate validation to, for example, a mobile network operator.

THE RMA TO ENSURE STANDARD COMPLIANCE OF SOFTWARE RADIOS

Security and reconfiguration management are preconditions to permit global circulation of SDR terminals. Current regulatory requirements (as described in [5]) are as such that every new configuration of hard and software must be approved by a responsible authority (i.e. must be type approved). So far this was a rather lengthy process, which would prevent the sensible commercial use of reconfigurable radio terminals. The RMA provides features capable to ensure that a responsible authority can have the final decision to whether a reconfiguration may go ahead or not, its structure is described in the subsequent section, followed by a report of its mechanisms.

The RMA – Network Part

The RMA is based on a distributed structure; its main parts are a 'configuration management unit', which is located within the reconfigurable/programmable terminal and a 'reconfiguration and software download support server', located within the network. The network resident 'Configuration Control Part' (CCP) executes those reconfiguration related functions and tasks that directly affect the network or the air interface, i.e. it controls and, if necessary restricts, those reconfiguration procedures that require the approval of the responsible authority (e.g. the network provider). The CCP provides the means to host this authority and provides a range of functions, these include:

a) reconfiguration software approval, provision, download negotiation and secure download,
b) evaluation, approval and assurance of standard compliance by implementing an intended terminal configuration, in a 'virtual configuration' process,
c) monitoring and control of configurations throughout the network,
d) provision of configuration rules for different reconfigurable radio platforms, and
e) registration of current/new terminal configurations.

To actually facilitate these tasks, there are a number of functional entities within the CCP (see Fig. 1, 'Configuration Control Part'): the AcA-Server performs most of the aforementioned tasks, it monitors the configurations of the network neighbourhood, with the aim to prevent mis-configurations, it manages the registration of terminal configurations, handles the software download and validates new configurations by executing a virtual configuration (VC) procedure [6] which ensures that the intended HW/SW combination (i.e. the new configuration) adheres to given standards. 'Rules & Policies' is a tool to be used by the network provider to specify certain platform dependent parameters (i.e. manufacturer dependent) and the reconfiguration policies of both the network provider and the end user (i.e. to implement the reconfiguration related contractual agreements between provider and user). The 'SW-Store' is a database hosting approved configuration software (OME versions or SW obtained from 3rd party providers) as well as the 'terminal configuration register'. The actual physical location of the CCP may be within the access but also in the core network (see also [6]).

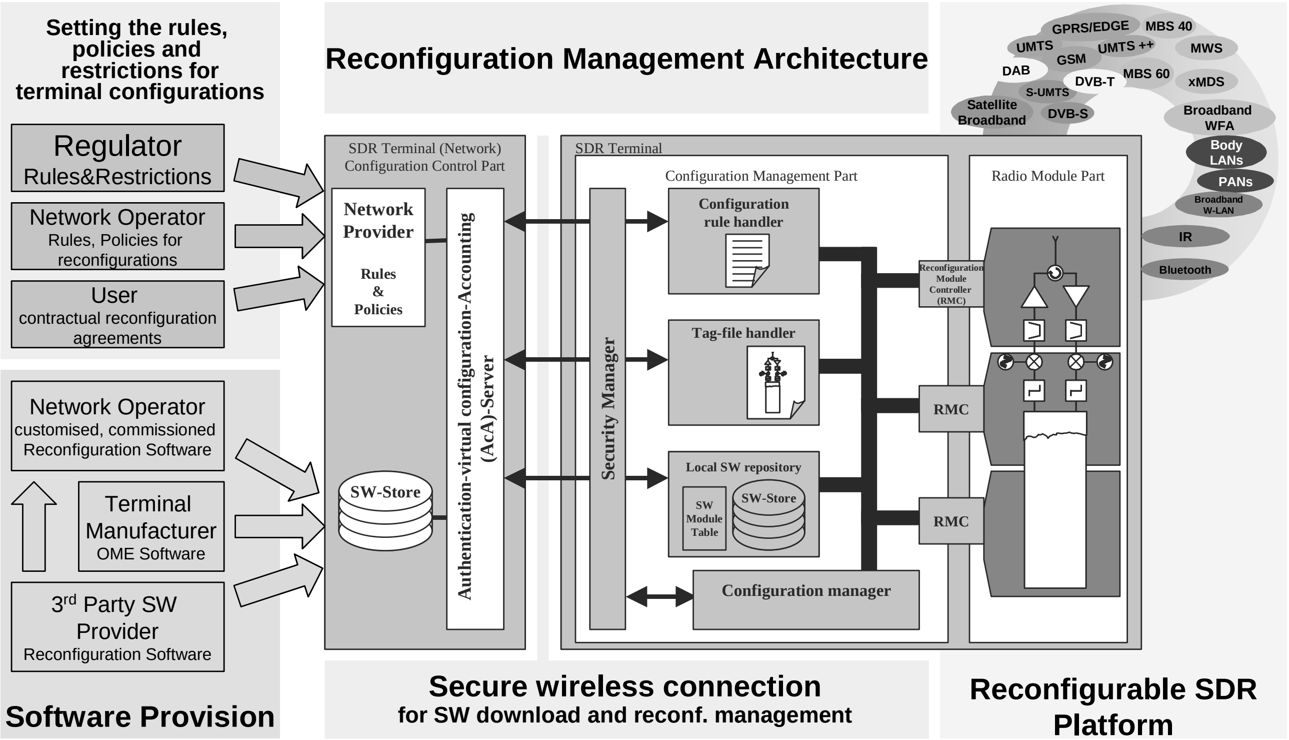
The RMA – Terminal Part

There are two parts of the RMA located within the reconfigurable terminal: a) the 'Configuration Management Part' (CMP) coordinates the configuration and reconfiguration processes of b) the configurable 'Radio Module Part' (RMP). Tasks of the CMP include:

a) the procurement of configuration software, using secure download and signalling channels,
b) handling of configuration rules, their storage, updates and interpretation,
c) generation and compilation of tag-files, using the details set in the rules and the configuration requests,
d) implementation of new configurations (i.e. installing the SW modules on the RMP execution platform), and
e) management of the reconfiguration related signalling.

The CMP contains a number of functional modules, firstly the 'Configuration Manager', which executes the reconfiguration sequences and manages the communication between the various modules within the CMP but also the external signalling, between CMP and CCP. A variable number of 'Reconfiguration Management Controllers' (RMC) acts as interfaces between the managing domain (i.e. the CMP) and the radio execution domain (i.e. the RMP). The task of the RMCs is to implement the actual configuration of radio modules within the RMP, controlled by the Configuration Manager module.

The other modules within the CMP include, a local software repository (to store radio configuration software), a configuration rule handler (this unit maintains the list of rules for reconfiguration, these rules depend on policies set by the network provider and also on the terminal type), a tag-file handler (to store, interpret, generate and alter tag-files) and a security manager (responsible for establishment, maintenance and termination of secure connections between the different management units and to prevent malicious reconfiguration requests and tampering during the download of reconfiguration software). A configuration software bus, based on CORBA, facilitates the transport of, as in objects wrapped, reconfiguration software between the parts of the RMA and the modules within the CMP; it also transports the signalling traffic within the CMP. The functions of the 'security manager' are required to ensure secure, trusted and authorised exchange/download of reconfiguration information and of configuration software between different parts of the architecture. N.B. specifications for security protocols are not included in this work, although it is envisaged that, due to different security requirements, security protocols of varying degrees of complexity/capability may be employed without impact on the architecture and the procedures outlined.



Setting the rules, policies and restrictions for terminal configurations
Regulator
Rules&Restrictions
Network Operator
Rules, Policies for reconfigurations
User
contractual reconfiguration agreements
Network Operator
customised, commissioned Reconfiguration Software
Terminal Manufacturer
OME Software
3rd Party SW Provider
Reconfiguration Software
Software Provision
Reconfiguration Management Architecture
SDR Terminal (Network) Configuration Control Part
Network Provider
Rules & Policies
SW-Store
Authentication-virtual configuration-Accounting (AcA)-Server
SDR Terminal
Configuration Management Part
Security Manager
Configuration rule handler
Tag-file handler
Local SW repository
SW Module Table
SW-Store
Configuration manager
Radio Module Part
Reconfiguration Module Controller (RMC)
RMC
RMC
Secure wireless connection
for SW download and reconf. management
GPRS/EDGE
MBS 40
UMTS
UMTS ++
MWS
GSM
DAB
MBS 60
DVB-T
xMDS
S-UMTS
Satellite Broadband
DVB-S
Broadband WFA
Body LANs
PANs
Broadband W-LAN
IR
Bluetooth
Reconfigurable SDR Platform

Fig. 1. Application of the RMA

The ‘Radio Module Part’ (RMP) hosts the actual execution platform of the software definable radio. One aim of the RMA was to define it in a way, that the terminal manufacturers still define their own platforms; the RMA facilitates this by providing a generalised reconfiguration management structure without specifying the required underlying hardware platform. This is achieved by introducing a dual state machine based interface between RMA and SDR Platform (see the RMCs in Fig. 1), hereby the terminal manufacturer implements the RMP side of the RMC’s.

Mechanisms within the RMA

The principle of the RMA is based on the mere requirement, that terminal configurations should be evaluated with a minimum of signalling and software download traffic, additionally this validation procedure should allow the use of self-obtained configuration software, to facilitate an open, competitive market for radio configuration software. Based on these assumptions, the mechanisms of the RMA are using a ‘tag-file’ (i.e. the blue-print of a radio) to evaluate whether an intended configuration complies to the radio standards, rather than up- and downloading the complete software for a radio implementation.

The mechanisms of the RMA are can be shown in an example reconfiguration process: Assuming a user who wants to install a new version of a radio software, obtained from a third party vendor, on their terminal. Whereby the user is aware of type, name and location (URL) of the software module. The user initiates the reconfiguration sequence by requesting a secure connection to their associated AcA (Authentication, Virtual configuration, Accounting) server, i.e. the configuration manager (CM) requests the security manager (both within the CMP) to establish this connection. After this initial authentication procedure, the CM forwards the actual reconfiguration request message and the AcA evaluates the validity of this request. If the request is valid, the AcA obtains the rules and policies applying for reconfiguration of this particular terminal (i.e. checking terminal- and operator/user contract- policies) and confirms (or declines) the validity of the requested reconfiguration. In case of a valid request, the AcA notifies the CM to continue with the reconfiguration sequence by testing whether the required software module is already resident within the terminals Local Software Repository (LSWR) or whether the SW module should be downloaded via the AcA. Once all required SW modules are available within the LSWR, the CM requests, from the TFH (tag-file-handler), the compilation of a new tag-file, describing the intended configuration (i.e. a script defining the use of software modules and structure of the software to implement the radio). The TFH takes (from the terminal resident Configuration Rule Handler/CRH) the set of implementation rules and from the LSWR, information about the software module/s and compiles the required new tag-file. Following this compilation, the CM forwards the tag-file to the AcA, which uses this description to virtually implement the intended radio configuration in its own virtual configuration (VC) process. Since reconfiguration software can only be downloaded via the AcA, only the tag-file will be passed back from the terminal to the network, to evaluate the standard compliance of the intended configuration (HW/SW combination), limiting the amount of data to be transmitted between reconfigurable terminal and network.

If the VC procedure acknowledges the standard compliance of the intended configuration, the AcA will inform the CM and the terminal can proceed with the reconfiguration sequence. The process finishes with a network registration of the new configuration and the termination of the secure reconfiguration connection.

SUMMARY

Situations or scenarios requiring a terminal or network initiated reconfiguration of a SDR terminal, may occur at any time. The actual need to reconfigure a mobile terminal may arise because of changing network conditions or new requirements of applications/users, this includes varying bandwidth/changing QoS demands, etc. To be able to gain from the flexibility reconfigurability offers to software definable/programmable terminals but to remain always in the limits regulation has set, it is crucial that a reconfiguration managing structure is in place. The architecture introduced, facilitates that a regulator can delegate validation to, for example, a mobile network operator, thereby allowing an open market in downloadable software to develop. Such an environment will encourage innovation in applications and capabilities (cf the open market in i-mode content in Japan).

New business models and new revenue streams for operators, service providers and software vendors are likely to emerge, eg the operator may charge the software provider (a small charge) for each validation instance of his software. This allows software providers to sell directly to end-users over the Internet, whilst the RMA provides the technical framework for strong control over the quality and performance of the software-hardware-network combination.

The RMA has been presented to the SDR Forum as part of its security and architecture work.

ACKNOWLEDGMENTS

The work reported in this paper has formed part of the Software Based Systems area of the Core 2 Research Programme of the Virtual Centre of Excellence in Mobile & Personal Communications, Mobile VCE, www.mobilevce.com, whose funding support, including that of EPSRC, is gratefully acknowledged. Fully detailed technical reports on this research are available to Industrial Members of Mobile VCE.

REFERENCES

[1] Tuttlebee WHW, *Advances in Software Defined Radio*, to appear in a Special Issue, on Software Radio, of the Annales de Telecommunication, to be published in June 2002.

[2] Mitola J, *Software Radio Architecture – Object-Oriented Approaches to Wireless Systems Engineering*, Wiley-Interscience, ISBN: 0-471-38492-5, 2000.

[3] Bing B, Jayant N, *A Cellphone For All Standards*, (a top level introduction to the features of SDR terminals), IEEE Spectrum, pp. 34-39, May 2002.

[4] Tuttlebee WHW ed., *Software Defined Radio: Origins, Drivers and International Perspectives*, John Wiley & Sons, Chichester, 2002.

[5] SDR Forum response to the FCCs ROI on Software Radio Technology, September 2001.

[6] Moessner K (ed), *The Mobile Soft Terminal – Form and Function*, Mobile VCE internal report, to be submitted in September 2002.