



Wireless World Research Forum
Working Group 6 White Paper
*Scenarios, system requirements and roadmaps for
reconfigurability*



About this document

This document constitutes a white paper developed within WG6 of WWRF, concerning scenarios, requirements and roadmaps for reconfigurability.

Scenarios, System Requirements and Roadmaps for Reconfigurability

Joint Editor Group:

George Dimitrakopoulos, University of Piraeus, Greece, gdimitra@unipi.gr

Flora Malamateniou, University of Piraeus, Greece, flora@unipi.gr

Karim El Khazen, Motorola Labs, Paris, karim@motorola.com

Didier Bourse, Motorola Labs, Paris, didier.bourse@motorola.com

Stephen Hope, Orange, stephen.hope@orange.co.uk

Abstract:

The migration of communications towards the Beyond the Third Generation (B3G) era has brought about the need for reconsidering typical aspects of communication technologies. The concept of reconfigurability, in particular, depending on the cooperation among diverse Radio Access Technologies, has incurred loads of research effort. This white paper presents typical scenarios that are envisaged to occur in a reconfigurability context, in order to extract the system requirements that should be taken into account by researchers. In addition, aspects on the commercial vitality of reconfigurability are also considered, as well as the respective technology roadmaps.



Table of Contents

1	Introduction	7
2	Application Scenarios for Reconfigurability.....	9
2.1	Introduction	9
2.2	Methodology for Scenario Analysis.....	9
2.2.1	The Process	9
2.2.2	The Actors	10
2.2.3	The Actors and Their Roles	11
2.3	Analysis of E ² R High Level System Scenarios.....	13
2.3.1	Family #1: Ubiquitous Access	13
2.3.2	Family #2: Pervasive Services	14
2.3.3	Family #3: Dynamic Resource Management.....	17
2.4	Scenarios Evaluation	20
3	Identification of System Requirements.....	21
3.1	Overall approach	21
3.2	Methodology for the extraction of requirements.....	21
3.2.1	Definitions.....	21
3.2.2	Characteristics of Requirements.....	22
3.2.3	Identification of a Requirement.....	22
3.2.4	Levels of Priority.....	22
3.3	High level system requirements deriving from the scenarios	23
3.3.1	Service Level Agreement.....	24
3.3.2	Equipment Reconfiguration	24
3.3.3	Security.....	26
3.3.4	No Radio Interference	28
3.3.5	Download	28
3.3.6	Reconfiguration Management.....	29
3.3.7	Service Adaptation	30
3.3.8	Vertical Handover	31
3.3.9	Service Provision.....	31
3.3.10	System Monitoring.....	32
3.3.11	Dynamic Resource Management	32
3.3.12	Spectrum Transfer	33
3.4	Conclusions	34
4	Roadmaps for Reconfigurability	35
4.1	Introductory approach	35
4.2	Business Models.....	35
4.3	The Responsibility Chain Concept.....	37
4.4	Reconfigurability Roadmaps.....	38
5	Conclusions	43
6	References	44

List of Figures

Figure 1: Scenarios Analysis Process.....	10
Figure 2: Ubiquitous Access: Mr. Rossi moves from Europe to USA	14



Wireless World Research Forum
 Working Group 6 White Paper
Scenarios, system requirements and roadmaps for reconfigurability



Figure 3: Pervasive Services: The Business Group in the Train..... 15
 Figure 4: Actors in End-to-End reconfigurable Systems36
 Figure 5: Deployment Roadmaps for Incremental Introduction of Reconfigurability Applications
 39

List of Tables

Table 1: Table of Actors..... 11
 Table 2: Capabilities List23



Wireless World Research Forum
Working Group 6 White Paper
Scenarios, system requirements and roadmaps for
reconfigurability





1 INTRODUCTION

As globalization penetrates in all fields of human initiative, the world of telecommunications is currently undergoing some radical changes, in order to meet the –continuously increasing – user demands. Utmost research interest is thus placed on Wireless communications, as a mean of transferring information quickly, easily and securely. Wireless Communications comprise nowadays a multiplicity of Radio Access Technology (RAT) standards, the most commonly used being GSM (Global System for Mobile communications) [i], GPRS (Generalized Packet Radio Service) [ii], UMTS (Universal Mobile Telecommunications System) [iii], BRANs (Broadband Radio Access Networks) or WLANs (Wireless Local Area Networks) [iv, v, vi] and DVB (Digital Video Broadcasting) [vii]. Moreover, this set of discrete technologies is currently transforming to one global infrastructure, called *Beyond the 3rd Generation* (B3G) wireless access infrastructure, aiming at offering innovative services, according to user demands, in a cost efficient manner. Major contributors towards this convergence are the *cooperative networks* [viii], [ix] and the *reconfigurability* [x] concepts.

The cooperative networks concept assumes that diverse technologies, such as cellular (2.5G/3G mobile networks), BRAN/WLAN and DVB systems can be cooperating components of a heterogeneous wireless-access infrastructure. This implies that a network provider (NP) can rely on more than one RAT, for the encountered specific conditions (e.g., hot-spot situations, traffic demand alterations, etc.) at different time zones and spatial regions. At the same time, a NP may also cooperate with other NPs, in order to have alternative solutions for maximizing the offered QoS levels. Advanced management functionality is required for supporting the cooperative networks concept. The required functionality deals with the allocation of traffic to the different RATs and networks, as well as with the allocation of applications to QoS levels. Relevant research attempts have been made in the recent past ([xi],[xii],[xiii],[xiv]).

Reconfigurability is an evolution of Software Defined Radio [xv]. It aims at bringing the full benefits of the valuable diversity within the radio eco-space, composed of a wide range of systems such as cellular, wireless local area and broadcast. More specifically, reconfigurability provides essential mechanisms to terminals and network segments, so as to enable them to adapt dynamically, transparently and securely to the most appropriate RAT [xvi]. Through reconfigurability, we can envision network segments that change RAT, in a self-organized manner, in order to better handle the offered demand. In this context, reconfigurability also supports the dynamic allocation of resources (especially spectrum) to RATs [xvii].

This white paper aims at providing the basic research framework towards a successful deployment of composite reconfigurable networks. For this purpose, special attention must be placed upon the concept of reconfigurability, in terms of the technology battlefields, in which innovative technologies must be recruited. Consequently, the structure of this white paper can be outlined as follows:

The next section introduces distinct families of application scenarios aggregating technical, business and regulatory visions. The scenarios presented are grouped in three main families representing a common thematic and corresponding to an anticipated coherent timeframe of



Wireless World Research Forum
Working Group 6 White Paper
*Scenarios, system requirements and roadmaps for
reconfigurability*



technical availability. Such scenarios are envisaged to occur in an end-to-end reconfigurability context and are essential in order to extract the basic requirements for reconfigurable systems. Section 3 contains the system requirements for the realization of reconfigurability and capabilities resulting from the scenarios which have been presented in the previous section. For this purpose, the respective methodology is described and then, the different capabilities of the reconfigurable system are identified. Each capability is refined to extract the associated requirements.

In addition, section 4 elaborates on the relevant technology roadmaps and business paths, while the last section presents the conclusions of this white paper research and some future work aspects.



2 APPLICATION SCENARIOS FOR RECONFIGURABILITY

2.1 Introduction

In order to have a clear view on the needs of reconfigurability, attention must be placed upon typical application scenarios envisaged to occur in a reconfigurability context, depicting diverse facets of reconfiguration.

Following analysis of the presented scenarios three main families of scenarios have derived:

- (1) Ubiquitous Access
- (2) Pervasive Services
- (3) Dynamic Resources Provisioning

The scenarios in each family have then been reviewed in greater detail and a common scenario for each family has been created by integrating the key elements of each contributed scenarios into one.

In addition, a further analysis has been carried out to identify the actors involved in the scenarios and the detailed interactions of those actors so that direct links can be established with the business models. The practicalities of implementing such scenarios from both the operator viewpoint and that of the user are also discussed.

2.2 Methodology for Scenario Analysis

2.2.1 The Process

The purpose of this analysis is to define scenarios in order to illustrate E²R requirements and constraints reconfigurations and to derive scenarios that capture the key reconfigurability elements. Figure 1 lists the main steps of the analysis process.

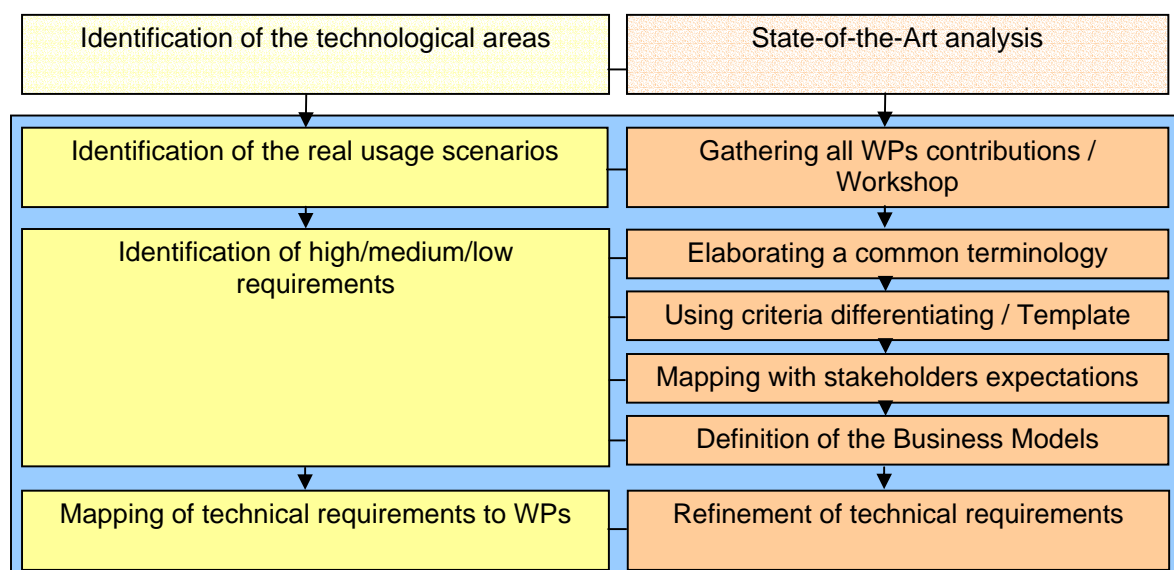




Figure 1: Scenarios Analysis Process

The first objective is to identify the main technological areas and to derive scenarios that capture the key reconfigurability elements. The next step is to clearly identify the different actors involved and the relations between these actors. Scenarios will be supported by a story described firstly as a script. This story will be used to identify the actor of the system as well as main objects of the system (e.g. networks elements, application platform...) involved in the reconfigurability process. Interactions and relations in between actors will be identified. The actors involved in the process are identified and the relationships between the actors are also reviewed. After further analysis, it will lead to the definition of the business models. The defined scenarios will be analysed from various points of view to extract the corresponding requirements, business models and provide inputs for others WPs in order to refine the technical requirements.

2.2.2 The Actors

In order to identify who constitutes an Actor in the end-to-end scenarios, it has been proposed that a separate actor should be considered whenever the functions associated to it may be performed by an independent entity completely separated from the rest of entities in the system. Similarly, if different functions are always performed by the same entity it is proposed that those functions are grouped in one single actor.

Based on this principle, the actors involved in the end-to-end scenarios are identified in the Table 1. However, before listing all the identified actors, it is interesting to provide clarification on differentiations of some actors (such as user and subscriber, network operator and service provider) and considerations on the different approaches related to the global roaming.

User v/s Subscriber

The traditional situation is that the user and subscriber is the same person but it is possible, in certain cases, that the person making use of the terminal (user) is not the same one as the one who has contracted services with a service provider or network operator (subscriber). This is quite common where the Terminal User is one of many on a corporate talk plan. In this case, the company is the subscriber who pays the bill and may dictate a policy regarding the potential reconfiguration of its terminals. Therefore, user and subscriber are separated to cover the maximum number of cases and not to limit the scope of the future business models.

Network Operator v/s Service Provider

The same situation happens with Network Operators (NOs) and Service Providers (SPs). NOs will continue to be strong SPs but the possibility also exists of a SP who does not own a network infrastructure and just signs agreements with one or more operators in order to serve its users. Therefore, they are considered as separate actors. This is strengthened by the fact that in the traditional model, the SP had been purely a reseller of airtime but now the the role of the SP is sometimes extended. In this case, not only airtime is provided but also mobile multimedia applications, content and other value added services in which the SP's brand is projected potentially in competition with that of the Network Operator. Potential brand erosion and revenues decrease could be key concerns for the Service Provider Network Operator.



Considerations regarding the Global Roaming

In order to achieve a global roaming, the potential provision of a Pilot Channel has been the subject of much discussion in the reconfigurability arena. There are some practical concerns as to how truly reconfigurable equipment would be able to communicate with the network environment on switch on or after, e.g. a battery failure in order to identify which network technologies are present and receive a download of the appropriate Radio Software for reconfiguration.

Various approaches have been suggested:

- The terminal could always have a default load stored in memory to which it can revert which may vary according to the main market in which the terminal was originally sold.
- The user could be able to take the terminal to a kiosk where an appropriate load of software may be delivered by a de-facto standard radio interface such as Bluetooth.
- A Global Pilot Channel Infrastructure could be provided to which handsets revert on switch on to receive network information and provide software download information. The implementation of such an infrastructure would be a significant undertaking and could be provided by a 3rd Party either on behalf of the Government/EU or directly or indirectly by a conglomerate of the interested operators. If such a step were mandated by say the EU it could seriously undermine the Business Case for SDR. However even though an Operator solution is the most likely the Pilot Channel Provider should not be ruled out of the list of Actors.

2.2.3 *The Actors and Their Roles*

The Table 1 groups the actors identified in the various E²R scenarios and gives a common definition of their roles.

Table 1: Table of Actors

Actor	Role
USER	A user is an entity, which uses services (e.g., 3GPP System services). Example: a person using a 3GPP System mobile station such as a mobile phone.
SUBSCRIBER	A subscriber is an entity (associated with one or more users) that is engaged in a subscription with a service provider. The subscriber is allowed to subscribe and unsubscribe services, to register a user or a list of users authorized to enjoy the services, and also to set the limits relative to the use of these services by the associated users.
RECONFIGURABLE EQUIPMENT	A reconfigurable equipment is a device used by the user/network operator to obtain/provide access to the communication services, and that can be modified with several kinds of reconfiguration processes. In case of an end-user reconfigurable equipment, it may be provided to the user by the service provider or the network operator, or directly acquired by the user. A reconfigurable equipment is autonomous and able to decide/act without any other actor intervention. Besides, it is aware of its context and self-aware (knowing its characteristics). Different classes of reconfigurable equipments will be considered.
EQUIPMENT MANUFACTURER	The equipment manufacturer is responsible for the design and manufacturing of the equipment (such as mobile devices, access points or base stations...) used in the service provision, network and user domains.



Wireless World Research Forum
 Working Group 6 White Paper
Scenarios, system requirements and roadmaps for reconfigurability



NETWORK OPERATOR (NO)	A network operator provides radio resources, mobility management and fixed capabilities to switch, route and handle the traffic associated with the services offered to users. Network capabilities are provided on behalf of service providers. A network operator may use several radio access technologies (e.g. GSM/GPRS, UMTS, IEEE 802.11x, DVB...) to provide these services to end users.
(VALUE ADDED) SERVICE PROVIDER (VA-SP)	A service provider is responsible for providing a service or a set of services to users associated with it. A service provider negotiates with network operators for network capabilities needed to provide services to its users. A value added service provider (VA-SP) supplies services for which additional charges may be incurred. A VASP can be considered as a SP with which the user contracts specific services not offered by the home service provider.
REGULATOR	A regulator sets laws and guidelines that determine the operation of the whole system. This includes aspects such as the acceptable equipment behaviour (regarding frequencies, power, etc.), the tests that must be passed in order to place equipment in the market, and the allocation of spectrum.
PILOT CHANNEL PROVIDER (PCP)	If available, the pilot channel provider coordinates the RAT discovery. It allows the terminal to discover the new radio interface to use and provides access to the software for the local systems.
CONTENT PROVIDER	A content provider creates and maintains multimedia repositories and makes them available to service providers or end-users through the service provider.
SOFTWARE PROVIDER	A software provider supplies the software to be downloaded and installed in network equipment or end-users terminals.
SERVICE AGGREGATOR	A service aggregator mediates between SPs/VASPs, operators and users. It keeps users aware of the available services, categorizes services depending their content, localization, terminal capabilities and subscriber profile, by operating a software platform for service, reconfiguration management and provision. The service aggregator comes into business level agreements with network operators and VASPs.
CERTIFICATION ENTITY	The Certification Entity guarantees the conformance of the protocol implementation and integrity of the software and the authenticity of its origin. Under the supervision of a regulator, this actor will be responsible for issuing, revoking and managing security credentials and public keys for data encryption and signature. This role can also be undertaken by an operator or a manufacturer or a third party.
SPECTRUM MANAGER	The spectrum manager is the entity responsible for approving and monitoring spectrum allocation to different entities and the transfer of spectrum between them (be it sharing or rental), so that operators comply with the rules set by the regulator.
RECONFIGURATION MANAGER	The reconfiguration manager is responsible for the reconfiguration management, intra/inter domain reconfiguration policy and respective interactions between service aggregators, certification bodies, operators, manufacturers...
SECURITY ENTITY	A security entity provides the security reconfiguration information and the security context for the system, in cooperation with the rest of the actors of the system.

Note that some actors may be regrouped later during the requirements capture and the elaboration of the business models: one actor may have one or several roles.



2.3 Analysis of E²R High Level System Scenarios

Three typical scenarios which cover all the reconfigurability aspects were identified:

- Ubiquitous Access
- Pervasive Services
- Dynamic Resources Provisioning

2.3.1 Family #1: Ubiquitous Access

Objectives of the Scenario

Ubiquitous Access scenario relates to the support of the user who switches on his device in a new wireless environment to which he has not been previously connected, e.g. when leaving an aircraft and seeking access to his services. Roaming is a particular example of this scenario, and the increase of roaming possibilities granted by the reconfigurability is highlighted.

Scenario's Concept

Customer A moves from Europe to USA (e.g. San Diego), Japan (e.g. Tokyo) or to China (e.g. Beijing), or vice versa, with an E²R reconfigurable equipment. Before departure, the E²R equipment is configured on a GSM/GPRS/EDGE mode or UTRA mode. Arriving at destination, the customer A switches on the E²R reconfigurable equipment and the local new system has to be activated and/or downloaded and configured on it. For example, considering San Diego, if it is present an IS95 or CDMA 2000 coverage, at least one of these radio interfaces have to be activated and/or downloaded and ready to be executed for service. Considering China, Narrowband TDD has to be activated and/or downloaded and ready to be executed for service, etc.

Reconfigurability Issues

Mr. Rossi is leaving his home in Turin during a secure download of his new e-mail messages with his E²R equipment. When he enters in his car, he starts – without interrupting the download – a conversation call with his office. During the journey to the airport, the download ends and the E²R equipment begins reading the subject of each new e-mail message: Mr. Rossi, with a vocal command, may order the E²R device to read the entire message or not.

When Mr. Rossi arrives close to the airport, the E²R device informs him that the car parking has free space at the fourth floor. After parking the car, Mr. Rossi moves inside the airport. Immediately, the E²R equipment informs Mr. Rossi with a particular vocal message that in the airport an automatic tele-check-in system is available. Therefore, Mr. Rossi downloads the tele-check-in client software and then performs the check-in operation with his E²R device, digiting his ticket-code on the E²R equipment and choosing his seat and his menu for the lunch. Moreover, Mr. Rossi personalises his “Personal Profile” in the tele-check-in system server to automatically choose that menu for the next times. Mr. Rossi leaves the baggage in a dedicated area of the airport. During the wait for the boarding, Mr. Rossi downloads with his E²R device the new lesson of his Electronic Advanced English Course and starts learning the new subjects, using his E²R equipment. When Mr. Rossi enters the airplane, he switches off his E²R device.

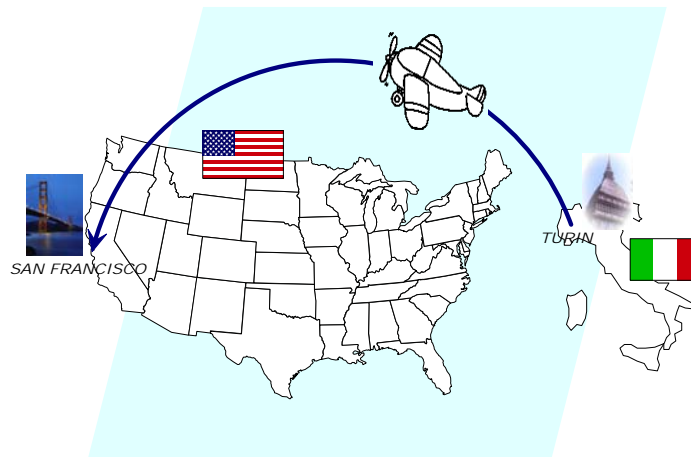


Figure 2: Ubiquitous Access: Mr. Rossi moves from Europe to USA

Arriving at San Francisco, Mr. Rossi switches on the E²R device that starts seeking for a cellular system. Since in USA the local system is different from Europe, the E²R reconfigurable equipment automatically begins a download of the new standard using the pilot channel given by the Pilot Channel Provider covering San Francisco airport. The Pilot Channel Provider, before starting the download, performs a security check with the Reconfiguration Manager, in order to know if Mr. Rossi “User Profile” has the “Standard reconfiguration” option enabled. After the download, the E²R reconfigurable equipment is able to manage all the services and applications supported by the new radio standard.

While Mr. Rossi is waiting for his baggage, he calls his wife using his E²R device, using a vocal command to activate the call. Then, he starts downloading new e-mail messages with his E²R reconfigurable equipment and, at the same time, books a car for his stay in USA. Then, Mr. Rossi moves to the hotel.

2.3.2 Family #2: Pervasive Services

Objectives of the Scenario

The purpose of this scenario is to stress the need for reconfigurability when several radio access technologies are present in the wireless environment. Indeed, to properly use these different access technologies, the reconfigurable equipment need many capabilities like system discovery, protocol reconfiguration and vertical handover. Besides, the reconfiguration of codecs, cipher algorithm is highlighted in this changing wireless environment. Transport scenarios is a good example to illustrate the reconfigurability with numerous radio technologies; besides, the applications and services which can be offered in transportation underline the emergence of value-added service providers (VASPs) which provide services other than classical telecommunications services.

Scenario's Concept

In a continuously changing environment (like a train, a plane...), new VASPs deploy innovative services (downloadable, web-based, reproduction, multimedia etc.). The VASPs do not own



network infrastructure so in order to demonstrate their services, they may come in contact with existing mobile operators with service aggregators or directly offer their services to the users. A VASP comes in agreement with an operator which gives him the possibility of direct renegotiation depending on the success of the provision of the service in question as well as the attractive percentage from the resulting revenue. In order to gain publicity, the various VASPs usually deploy different versions of a service in terms of terminal capabilities and tariff demands.

In such a telecommunication environment, a company group travels by train to another city for an important meeting. The colleagues are discovering, using their E²R reconfigurable equipments, the different access technologies though their way (e.g. WLAN, GSM, UMTS...). They may use the company groupware software while on the move, while their equipments may communicate through a wireless or a mobile operator to the company intranet. The complex and continuously changing telecommunication environment may require vertical handovers, capability negotiation, situation-awareness and the possibility to adapt the services based on telecommunication system context parameters and restriction, as well as to reconfigure the Reconfigurable Equipment with new protocols, codecs, and cipher algorithms for example. Multimedia location-based services related to tourist content and information on the visited areas are also available to the users through intelligent service provisioning of VASPs (dynamic end-user application discovery and adaptation, reconfiguration policy provision, charging).

Reconfigurability Issues

In such a telecommunication environment, Ms Eve and other employees of a large company, after a working day, leave straight by train for another city. As soon as they embark on the train, they continue their meeting preparation work, using their company groupware software and have access to their Company Intranet using their E²R reconfigurable equipment. Private communication between Eve and her colleagues takes place thanks to a secure WLAN ad-hoc mode between corporate laptops. Moreover, Eve's equipment (e.g. laptop), the more powerful, becomes the gateway (and proxy) of her group towards the station's WLAN facility. During the journey, every passenger has the possibility to use the WLAN offered inside the train with an extra and rather expensive charging but also with the choice to get multimedia type information regarding the final or the mediate destinations and interesting points along the way (services provided by a VASP).

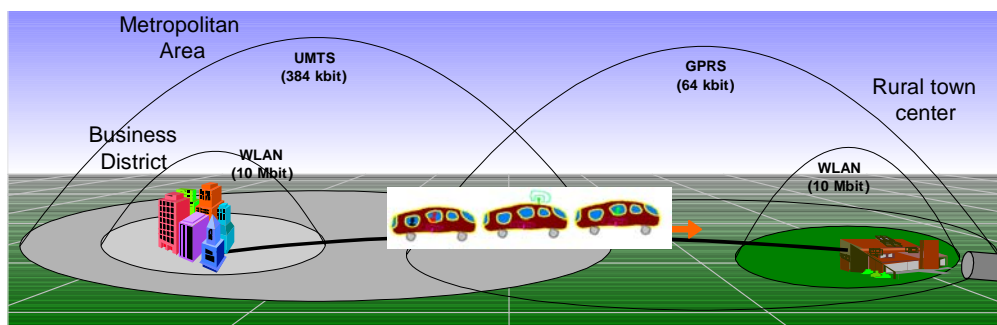


Figure 3: Pervasive Services: The Business Group in the Train



Wireless World Research Forum
Working Group 6 White Paper
*Scenarios, system requirements and roadmaps for
reconfigurability*



The multi-band reconfigurable equipment of Eve's is monitoring/interpreting context information continuously and is able to select a system to connect in a personalized way: the system selection may be carried out according to the various profiles (user/tariffing demands and terminal capabilities). For the system monitoring, new agents (mainly proprietary) may be discovered, downloaded/installed and executed. Protocol downloading and reconfiguration may take place in order to avoid frequent vertical handovers and also provide soft switching between access systems. When the WLAN connectivity breaks as the train leaves the station and speeds up, the Eve's equipment has already discovered an alternative radio access technology: UMTS. The handover takes place with information derived from Eve's profile regarding acceptable charging etc. In case that this information is deficient, the software agent which manages her connection notifies Eve about the new charging and the estimated cost. The vertical handover results to protocol downloading, installing and execution or to a new protocol release update. Furthermore, different handover algorithms may be employed (standardized or proprietary) in order to minimize packet loss and handover delay and to ensure service continuity (avoid inter-system handover).

Eve and her boss at company headquarters are communicating through a videoconference (services provided by a VASP or directly by the network operator). When she was under WLAN coverage, she experiences an excellent Quality of Service. However, after seamless handover to UMTS, the quality was automatically decreased to black and white video, with a smaller image size. Nevertheless the quality of the transmission is still acceptable. This is enabled through reconfiguration of the codecs within Eve's equipment and activation of suitable transcoders placed in appropriate network nodes.

During the journey every passenger has the possibility to use the WLAN offered inside the train with an extra charging but also with the possibility to get multimedia type information regarding the final or the mediate destinations and interesting points along the way. Such demanding multimedia services may trigger reconfiguration to codecs/transcoders while enhanced display analysis may trigger reconfiguration to new drivers available (standardized or proprietary). Additionally, new reproduction programs may be needed or new versions of already installed ones.

After the train has left the first mediate station Eve's agent receives a report from the hotel's system about a problem with the booked rooms. Because of bad weather a group will not leave the city and thus the hotel must book rooms to another hotel. Eve's agent sends the profiles of the group so that the hotel will find rooms to other hotels (same stars, same facilities). The hotel sends two alternative hotels (that is a list with description of the hotels, photos and possibility for virtual presence in each one) Eve is notified about the problem and after a short discussion among the colleagues the agent notifies the hotel about the decision.

Finally, Eve and her boss close the discussion having agreed on the final version of the file. Due to the location, the high mobility and congestion, the network establishes 2 links, UMTS and GSM (respective reconfiguration is performed) in order to support the service requirements executed by the users for example when Eve shares the final document with her boss. She also shares the final version with her colleagues in the train thanks to the WLAN ad-hoc connectivity.



Wireless World Research Forum
Working Group 6 White Paper
*Scenarios, system requirements and roadmaps for
reconfigurability*



Eve's 12-year old daughter calls her and asks for help in her mathematics homework. Eve attempts to trigger establishment of a videoconference but receives a warning from her software agent that the provision of such a service in the current context would be much too expensive for her (even after optimization actions like adapting the service and reconfiguring the terminal to use another network), according to personal preferences stored in her profile. Her service provider uses an advanced charging system that ensures a distinction between business related and private communication charges (i.e. private/personal account Vs Company's account). Thus, Eve suggests to her daughter to have this session later, also given the fact that her expected time of arrival at the hotel is well before the usual bed time of her daughter.

Eve arrives at her destination and while she is reading her e-mails, the corresponding VASP announces (through appropriate automated procedures) availability of a new version of the messaging application with additional location-awareness features. Eve receives the whole description of the messaging application (since it is currently executing the service), and also information about pricing and purchase conditions. Despite a higher price, she opts to stop execution of the older version and to immediately download and execute the new one. The equipment starts the authentication process with information extracted from Eve's security profile, but the WLAN service uses different cipher algorithm which the terminal is incapable of, so after setting up a secure configuration channel the new cipher algorithm is downloaded and installed and the new messaging application can be download. The downloading process is also based on Eve's security profile.

Just before Eve closes the day, she receives a notification that certain bills must be paid in the next day but the web-banking server of her bank will be down due to maintenance actions. She immediately moves money to an alternative web-banking account and reconfigures her agent to use that in the cases of urgent payments.

2.3.3 Family #3: Dynamic Resource Management

Objectives of the Scenario

The case of dynamic cells traffic areas (e.g. unusual events such as sporting event, accident, natural disaster...) has a particular significance to illustrate the concept of dynamic resource management. The goal of this scenario is to underline that a dynamic reconfiguration of the terminal and of network elements improves the bandwidth for the users thanks to better adapted radio interfaces, additional spectrum... In this case, the protocol stack must be updated in the terminal and in the network. The different communication systems covering such areas, which can move, must adapt to the load and services variations. To dynamically face these changes of traffic and provide fast and cheap cells coverage to the reconfigurable equipment, the network operators would perform a spatial/temporal reconfiguration and/or redeployment of their networks capacities as well as a load balancing, based on different cooperation schemes.

Scenario's Concept

In summer 2008, the Olympic Marathon run will be held in Beijing. The route encompasses different kinds of areas: urban, sub-urban and rural areas, where a cellular infrastructure is



already deployed. However, this infrastructure was designed to handle classical traffic, corresponding to such areas and is unable to cope with the supplementary traffic generated by the marathon's followers. Moreover, this additional traffic is going to follow the run, e.g. requiring sporadic (in time) additional capacity on a given location. Such variation in traffic demand in space and time could be called "Dynamic cells".

Reconfigurability Issues

In this scenario, dynamic network planning and configuration are needed. For that purpose, state of the art solutions is to bring transportable infrastructure and to manually proceed to a local network planning, leading to a costly solution (involving people on the field) and sub-optimal solution (manual and local planning).

The reconfigurable networks equipments detect on their own the change in the traffic conditions, as well as the alternate radio access technology they could cooperate with on the same coverage. With the current network configuration the operator is not able to serve all the users. This does not necessarily means that the operator is not able to provide the service at all, but rather that the level of service does not match the one that may have been agreed, in a Service Level Agreement (SLA), between the operator and the user (which could be also a service provider if it is a separate entity from the network operator). So, in order to comply with the SLA, the network starts a reconfiguration process in the network infrastructure covering that area. As a result, the network has several possibilities:

- To reconfigure itself for tackling efficiently the incoming traffic demand by assigning more processing or spectrum resources in the base stations to certain radio technologies (such as 3G/HSDPA) which offer more bandwidth for data services, and therefore reducing the resources allocated to other technologies (such as GSM),
- To balance a part of its traffic into a cooperating network operator and/or radio technology (e.g. to use WLAN coverage when available, or balance traffic over GSM/EDGE/UMTS taking into account the requested types of service, etc...). For instance, the users making voice calls on UMTS could be moved to GSM, therefore freeing space for users that want to employ data services,
- To ask for additional spectrum for tackling the traffic demand. The operator could rent some spectrum blocks offered by other operators which have free portions of spectrum (or only rent part of their infrastructure) according to Regulators rules. This compliance with regulator rules may be ensured by the intervention of a dedicated entity (Spectrum Manager) that will cooperate with the operators in order to successfully carry out the spectrum transfer.

In any of the previous cases, it may be necessary for the E²R equipment to reconfigure in order to adapt to the new radio technology or to the new network configuration. If the E²R equipment does not have the necessary pieces of software for such a reconfiguration, a software download will have to take place in order for the equipment to get those pieces of software and install them. For instance, a GSM terminal should download the EDGE protocol stack before the network decides to switch from GSM to EDGE. In that case, the reconfiguration procedures encompass the radio access layer stacks. Reconfiguration could also be imagined in the core network to efficiently absorb the additional capacity brought by the enhancement of the radio interface.



Wireless World Research Forum
Working Group 6 White Paper
*Scenarios, system requirements and roadmaps for
reconfigurability*



The reconfiguration process will require the intervention of many different actors, but a relevant role will be performed by the reconfiguration manager. This actor will be responsible for the coordination between the different entities, the acquisition of the software modules to be downloaded and the provision of these modules to the network entities in charge of the actual download. Another relevant actor involved in the download process is the certification entity, who will guarantee the integrity and authenticity of the downloaded software, so the whole process is performed securely for both the network and terminal.

While the run is on-going, thousands of spectators are waiting for the first runner to enter the Olympic Stadium in Athens. Some spectators may still be accessing the stadium. One of the possible ways in which they obtained their tickets could have been through their mobile phones. In this case they do not need a physical ticket to access the stadium; the information needed to gain access is already stored in the terminal. When the spectator gets near the entrance gate, a communication is established between the terminal and the gate (through some short-range wireless technology such as Bluetooth), which checks if the terminal has a valid ticket stored. After the necessary tests, the gate determines the validity of the ticket and the spectator can access the stadium.

The spectators are following real time the evolution of the run thanks to a huge screen in the stadium or directly on their DVB-able devices. Real time video is provided over the stadium thanks to digital broadcast video. This again may require that some E²R equipments download the necessary software to be able to receive DVB. The operator may detect that a user is present at the stadium and send him/her a notice asking if they want to download the necessary software to be able to watch the video stream.

It must be noted the difference between “radio” software which allows the E²R equipment to reconfigure to a new radio access technology, and “application” software which may be for instance a special player to present the video stream to the user. In the first case, the layers affected by the reconfiguration are the first three (physical, link and network layers), while in the latter case it is the application layer the one that is modified. It also must be mentioned that a “radio” reconfiguration does not necessarily imply the complete modification of all the layers 1, 2 and 3. The reconfiguration may be as simple as a change in a frequency band or as complex as a change of the whole protocol stack from one RAT to another.

On the other side, the reconfiguration of the networks provides enough capacity to allow the journalists to stream the video directly from their camera to the TV mobile centre of operation, which act as a content provider in that case, merging the video streams with statistical figures and anecdotes gathered through a secure channel to their private database.

In addition to the DVB coverage, the stadium has been covered by WLAN type of connectivity which could be used to get side information not included in the DVB flow. For instance, Mr Dupont could follow the situation of his favourite runner (who is unfortunately a little bit slower than the other runners and has therefore disappeared from the DVB broadcast which focuses only on the leading group). People whose terminals do not have this capability could decide to



download the appropriate pieces of software to enable the combination of information delivered from various radio access technologies. In this case, two radio links are opened: DVB and WLAN.

When the leading group of runner enters the stadium, a sudden lack of capacity is appearing. Indeed, in addition to the journalist fleet (still making real time video and comments), the thousands of people in the stadium are starting to share the end of the run with their family by either sending SMS, MMS, videos thanks to their video/camera equipments or by instant messaging means (push-to-talk, push-to-view). All the legacy wireless systems are fully loaded; the only way to get additional capacity is to get additional spectrum allocation. For that purpose, the Regulator is contacted (or any entity representing the regulator). It identifies free pieces in the spectrum (part of band, potentially after spectrum de-fragmentation). Once notified, operators and users begin to use the new allocated spectrum.

2.4 Scenarios Evaluation

The aforementioned three families of scenarios represent a significant step forward in terms of identifying where reconfigurability can play a major role in the delivery of services to the user and also in the optimisation of the network resources to achieve the best results.

In addition, this analysis has highlighted potential new actors in the Communications Business Model such as the Software provider and also raises the issue to identify a common method to download the software over a reconfigurable device. An over-the-air approach, totally transparent to the user, could require a Pilot Channel available on a selected group of frequencies common in all the countries of the world. Otherwise, a kiosk model may be possible where software downloads can be obtained from a kiosk e.g. at international airports, train stations, hotels, etc. A mixed approach could be identified such as: a smart card or the terminal itself has in the memory several systems/standards and the activation can be generated via network input or via auto detection.

Less ambitious scenarios can also be considered. Instead of download a whole, new radio interface, the network operator or the user can simply upgrade the current radio interface in order to fix a bug or implement better algorithms in order to improve the network capacity. In some devices, it is not possible to reconfigure the lower layers, however new algorithms to improve the higher layers (cell selection...) can be downloaded. It is the network operator responsibility to choose a mass software upgrade or simply to notify the users who can choose to download these new functionalities or not.



3 IDENTIFICATION OF SYSTEM REQUIREMENTS

3.1 Overall approach

This section identifies system requirements and capabilities resulting from the scenarios which have been presented in the previous section. The requirements identified refer to reconfigurability issues and functions.

The first subsection describes the methodology. After that, the different capabilities of the reconfigurable system are identified. Each capability is refined to extract the associated requirements.

The end-to-end reconfigurability framework is distributed over various components of the system. For example, sub-parts of this system framework will be equipment, access point... Requirements consolidation is carried out at system level to take into account the different part of the systems and all types of reconfiguration.

Thanks to the scenarios and the associated requirements, the resulting achievement will be the system analysis. These requirements will help the respective research groups in their technological choices, specifications, etc.

3.2 Methodology for the extraction of requirements

Scenarios are of highest importance as they address all the subjects or point of view on the system. During the 1st stage of the analysis (Scenario Description), nominal scenarios have been described. During the 2nd stage of the analysis (requirements capture), requirements and capabilities are identified both for the nominal cases (as described in the scripts of the various scenarios) as well as for the malfunction or malpractice or malicious intents situations which may result from the exercise of such scenarios.

3.2.1 Definitions

The already conducted research has considered system capabilities and requirements:

- **Capabilities**, which represent a class of common characteristics or features that a system has to provide, for instance security, privacy, etc ...
- **Requirements**, which are linked to system capabilities, and provide an additional level of detail.

There are two types of requirements, technical and non-technical:

- **Technical Requirements** describe both the function of the system and the operational constraints within which this function is performed and include functional, performance, interface and quality requirements,
- **Non-Technical Requirements** cover other aspects such as contractual understandings, conditions and/or clauses, rules, etc



3.2.2 Characteristics of Requirements

Requirements should describe desired characteristics of the specified system functionality. It illustrates a characteristic of the problem not a solution. Solution will be studied later during the design phase. The major qualities of a requirement are:

- **Simple:** A requirement must have an elementary structure and state a basic need. It cannot, at a given level, be broken down into several simpler requirements. At system level, a simple requirement can be broken down into several requirements at Component level.
- **Concise:** A requirement must be expressed in a brief and clear manner. It contains neither an explanation nor a justification.
- **Unambiguous:** A requirement must have only one possible interpretation. A requirement is said ambiguous if it can be semantically interpreted in several ways, implying an uncertainty with regard to the design to be elaborated.
- **Verifiable:** As much as possible, it should be possible to verify requirements: if a test can not be associated, the validity of that requirement should be further investigated, requirements should be testable either by Inspection or Demonstration or Analysis or Test points, requirement can be refined in various (testable) sub-requirements to be testable, an effective finite procedure must make it possible to check that the system comply to the requirement.
- **Feasible:** It should be considered if a realistic and satisfactory technical solution can be implemented or can be elaborated in the timeframe of the project.
- **Non-redundant:** A requirement must have no overlap with another requirement. In case of redundancy, requirements must be divided and refined until suppression of the overlap.
- **Non-incompatible:** No conflict with another requirement (see above).
- **Classifiable:** It can be associated with an attribute belonging to a previously adopted classification system.
- **Necessary:** A requirement reflects a need.
- **Traceable:** Identifiable by a unique identifier.

3.2.3 Identification of a Requirement

Each requirement is identified in the following way: “**Capability Requirement**” where **Capability** is one word dedicated to express the corresponding capability, and **Requirement** is one word dedicated to express the corresponding requirement. Some explanations, description, example, and schema are added to help understanding of the capability or the requirement and support the definition.

3.2.4 Levels of Priority

Three levels of priority are defined for the requirements: mandatory, recommended or optional. These levels are indicated by the key words **SHALL**, **SHOULD** and **MAY** respectively. The meaning of the key words is taken from the RFC 2119 and quoted below:

- **SHALL** means “that the definition is an absolute requirement of the specification”.



- **SHOULD** means “that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.”
- **MAY** means “that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item.”

3.3 High level system requirements deriving from the scenarios

The Table 2 groups the requirements identified in a list of capabilities and provide a definition of each capability.

Table 2: Capabilities List

Capability	Definition
Service Level Agreement	A service level agreement permits the parties involved in it to establish the minimum performance criteria for service provision and the actions that will take effect if the service does not meet these criteria.
Equipment Reconfiguration	The equipment must be able to change its configuration including operating parameters by means of software (such as frequency, modulation or transmitted power autonomously or without any external maintenance.
Security	In case of upgrade of one or more elements of the system, the equipment reconfiguration must be performed securely.
No Radio Interference	Protection from the possible interference coming from badly reconfigured equipment must be provided.
Download	There must exist mechanisms that allow the equipment to obtain a software module and download it in order to reconfigure to a new configuration in a new wireless network.
Reconfiguration Management	The end-to-end reconfiguration control management actions are assumed to be carried out by a Reconfiguration Manager. The reconfiguration process might be initiated either by the user equipment or by the network. The Reconfiguration Manager is a virtual entity which is not required but is used in order to facilitate the expression of the requirements, it will be stated by the design phase of the project if this entity has to be created or not.
Service Adaptation	Active services can be adapted to changes in the network status (e.g. congestion) or modifications of the equipment (e.g. reconfiguration), or alteration of the access network used by a equipment (e.g. vertical handover). Service adaptation may cause reconfiguration in equipment in an attempt to avoid major disruption on the executed service.
Vertical Handover	Equipments are able to move through different access networks without losing their active connections. VHO can



	be equipment or network initiated.
Service Provision	Service provision refers to basic telecommunication services as well as value added services offered by operators or independent VAPs.
System Monitoring	The equipment and network must be able to monitor the current state of system operation (traffic, used spectrum, available technologies) in order to be able to estimate available resources and to facilitate the 'best' use of existing and available resources.
Dynamic Resource Management	The network operator is able to dynamically assign its resources to the different tasks to be performed in order to make the best use of them.
Spectrum Transfer	The owners of the spectrum are able to transfer their spectrum to other parties through commercial agreements such as a re-sale or a lease. Besides, in order to make new spectrum available, move an existing technology to a different band or change the technology currently assigned to a certain band the regulator may decide to perform a reallocation of the spectrum assigned to communication systems.

3.3.1 Service Level Agreement

Capability: Service Level Agreement (SLA)

A service level agreement permits the parties involved in it to establish the minimum performance criteria for service provision and the actions that will take effect if the service does not meet these criteria.

Requirement identification: **SLA_Establishment**

A service level agreement SHOULD be established between different parties in the system (e.g. User – Service Provider or Service Provider – Network Operator).

Requirement identification: **SLA_RoamingNO-NO**

A roaming agreement SHOULD exist between network operators.

Requirement identification: **SLA_RoamingUser-NO**

A roaming agreement SHOULD exist between user and network operators.

Requirement identification: **SLA_Download**

An SLA agreement SHOULD exist between the network operator of the subscriber and the entity responsible of the software download.

Requirement identification: **SLA_Software**

An SLA agreement SHOULD exist between the network operator of the subscriber and the software provider.

3.3.2 Equipment Reconfiguration

The reconfiguration software is software which modifies the operating parameters of reconfigurable equipment. The equipment profile is a set of rules representing distinctive features or characteristics of the user reconfigurable equipment. An equipment may have different profiles



defined by different actors such as user, manufacturer, network operator or service provider. The software repository is a database which contains the reconfiguration software.

Capability: Equipment Reconfiguration (EqptReconf)

The equipment shall be able to change its operation parameters by means of software (such as frequency, modulation or transmitted power) autonomously or without any external maintenance.

Requirement identification: **EqptReconf_Security**

The reconfiguration process SHALL be performed securely (see security capability).

Requirement identification: **EqptReconf_OtherApprove**

The reconfiguration software MAY require the approval of other actors in the system (such as network operator or service provider) before it is installed in the equipment.

Requirement identification: **EqptReconf_OperControlled**

The reconfiguration process of the network equipment SHALL be performed and controlled by the network operator.

Requirement identification: **EqptReconf_UserProfile**

User SHALL be able to configure the equipment profile to control the reconfiguration possibilities.

Requirement identification: **EqptReconf_OpenInterface**

Open interfaces SHOULD exist that allow third parties to develop reconfiguration software for reconfigurable equipment.

Requirement identification: **EqptReconf_Check**

It SHALL be checked that the reconfigurable equipment will support the new configuration before the reconfiguration process is initiated.

Requirement identification: **EqptReconf_Repository**

It SHALL be verified that the new software for the reconfigurable equipment exists in the software repository.

Requirement identification: **EqptReconf_Install**

After download, installation and configuration, the success of the process SHALL be verified.

Requirement identification: **EqptReconf_Interop**

After the reconfiguration the reconfigured equipment SHALL continue to interoperate correctly with the rest of the system equipment.

Requirement identification: **EqptReconf_Test**

After successful installation, a test SHALL be performed to check the new configuration; result of the test will confirm the new configuration (it could initiate a recovery process).

Requirement identification: **EqptReconf_Rollback**

In the case of equipment upgrade, the download SHALL be roll back to its previous configuration if the upgrade does not succeed.

Requirement identification: **EqptReconf_Recovery**

The reconfigurable equipment SHALL be able to return to a known stable configuration.

Requirement identification: **EqptReconf_Reset**

The reconfigurable equipment SHALL be able to return to the original configuration.

Requirement identification: **EqptReconf_Suspend**

At any time of the reconfiguration process, it SHALL be possible to suspend the process so it can be resumed later.

Requirement identification: **EqptReconf_Stop**

At any time of the reconfiguration process, it SHALL be possible to stop the process.



Requirements explanation

EqptReconf_Check, EqptReconf_Repository, EqptReconf_Install, EqptReconf_Interop, EqptReconf_Test:

In order to avoid a download/installation failure, several points must be checked:

- Firstly, the right version of the software module (corresponding to the user equipment type) must be found in the software repository.
- The new software to be installed must be compatible with other installed software.
- Besides, the equipment must have enough resource especially memory to support the new software. For example, if the user has already two radio interface on his equipment; it is possible that the equipment cannot accept a new protocol stack due to an insufficient memory.
- The equipment checks the result of the installation.

EqptReconf_Suspend:

In case of switch off or battery fail and if the process is “suspend” it will be possible to resume the process otherwise the process has been “stopped” and the equipment recover its previous features.

EqptReconf_Stop:

In case the user change of needs or the process failed or the process can not be suspended. In this case, the reconfiguration process cannot be resumed.

EqptReconf_Rollback, EqptReconf_Recovery, EqptReconf_Reset:

After the installation of new software in the reconfigurable equipment it may be desired to remove that software or to bring the equipment to a different state. There are several reasons for this:

- Rollback: A first one would be the case in which the reconfiguration process fails. In this case, it would be disastrous (for the NO and manufacturer image) that the user cannot recover to a stable state which would be preferentially the previous state. For example in the case of a UMTS to CDMA2000 upgrade, if the installation of the CDMA2000 protocol stack failed, the reconfigurable equipment should keep and recover the UMTS radio interface.
- Recovery: This could happen for instance when returning home after a trip (as is the case in scenario 1). In this situation the user will want to recover the configuration that he had before starting the trip. It can be possible to download again this configuration but it is more efficient to maintain this configuration in memory if possible.
- Reset: This would be the case in which the user wishes to return the equipment to its original state (i.e. the one the equipment had when it was first used) and not to one specific previous state as it is the case in recovery.

3.3.3 Security

Capability: Security (Security)

In case of upgrade of one or more elements of the system, the equipment reconfiguration shall be performed securely.

Requirement identification: **Security_Authentication**

In the case of reconfigurable equipment upgrade, the user/subscriber SHALL be authenticated.

Requirement identification: **Security_AuthenticationNet**



In the case of reconfigurable equipment upgrade, the Network SHALL be authenticated by the equipment.

Requirement identification: **Security_AuthenticationTerm**

In the case of reconfigurable equipment upgrade, the equipment SHALL be authenticated.

Requirement identification: **Security_Identification**

In the reconfiguration process, all parties involved SHALL be able to identify themselves to each other.

Requirement identification: **Security_Authorization**

The equipment SHALL be authorized to perform the reconfiguration process.

Requirement identification: **Security_Privacy**

The personal data, user profile and equipment profile stored in the reconfigurable equipment SHALL be protected from unauthorized access.

Requirement identification: **Security_Regulator**

There SHALL be a way for the regulator to be able to approve software.

Requirement identification: **Security_Certification**

It SHALL be possible to verify the origin of the software before the download is performed.

Requirement identification: **Security_Integrity**

The integrity of the software to be downloaded SHALL be verified before installation.

Requirement identification: **Security_SoftwareCorrect**

Proper operation of the software to install SHALL be guaranteed before installation.

Requirement identification: **Security_DetectProtection**

The detection-control mechanism implemented in the equipment SHALL NOT be modified by entities not authorized to do so (see *Interference_Control*).

Requirements explanation

Security_Authentication, Security_AuthenticationNet, Security_Identification:

Before the download of a reconfigurable software, the user should be identified (e.g. SIM, login/password...) for several reasons:

- To verify that the user has the right to download a new patch or interface,
- For billing purpose.

But it is important too for the user to trust the pilot channel provider and/or the reconfiguration repository. So, the network operator of the user should guarantee the software and the identity of the pilot channel provider and/or the reconfiguration repository.

Security_Regulator:

The requirement implies that there must exist a way for the regulator to approve software, not that this approval will be necessary for any or all software (that is the regulator's choice) For some critical types of software (e.g. new radio interface), it may be necessary to have a regulatory approval whereas for less critical software (vocoder...), it won't be necessary.

Security_Integrity:

The integrity of the software download should be guarantee for example at the end of the connection, the reconfigurable equipment and the software repository can verify a checksum on the downloaded software (e.g. MD5 checksum).

Security_Software_Correct:



This implies that the software has been tested and its correct behaviour has been verified. This can be done by different actors such as the software provider, the operator or a trusted 3rd party (or by all of them).

3.3.4 *No Radio Interference*

Capability: No Radio Interference (Interference)

Protection from the possible interference coming from badly reconfigured equipment shall be provided.

Requirement identification: **Interference_Disconnect**

A mechanism SHALL be provided to the network operator enabling the disconnection from the network of any equipment that is causing interference with other equipments or operating incorrectly, if it is impossible to correct this behaviour.

Requirement identification: **Interference_Transmit**

In the case of the current configuration of the equipment is not supported in a certain area, the reconfigurable equipment SHALL NOT start a transmission until it has received or gathered information on what frequency it is allowed to use.

Requirement identification: **Interference_Control** The reconfigurable equipment SHOULD include a detection-control mechanism which checks that the equipment is not causing interference, and if so is able to stop this incorrect behaviour.

Requirements explanation

Unfortunately, it is possible that the reconfiguration process lead to a bad behaviour of the equipment. This unexpected behaviour can be due to:

- A bug in the reconfiguration software,
- The new software that could be incompatible with the current configuration of the equipment,
- A malicious program: virus or trojan horse.

In this case, the manufacturer can implement a detection-control mechanism in the equipment (probably near the antenna) which checks that the radio emission of the user equipment is in conformance with the regulator limits. Otherwise, the network operator can monitor regularly the spectrum to detect interfering device.

3.3.5 *Download*

Capability: Download (Download)

There shall exist mechanisms that allow the equipment to obtain a software module and download it in order to reconfigure to a new configuration in a new wireless network.

Requirement identification: **Download_Approval**

A mechanism SHALL be implemented that enables to ask for user download approval before download.

Requirement identification: **Download_Billing**

There SHALL exist a mechanism that enables the software download to be billed to the user.

Requirement identification: **Download_SchedControl**



In case of a massive download, a mechanism SHALL be provided to the operator to perform the scheduling and control of the download process in order to avoid network congestion.

Requirement identification: **Download_Suspend**

At any time of the download process, it SHALL be possible to suspend the process so it can be resumed later.

Requirement identification: **Download_Resume**

It SHALL be possible to resume an interrupted download.

Requirement identification: **Download_Stop**

At any time of the download process, it SHALL be possible to stop the process.

Requirements explanation

Download_Approval:

Depending on user-profile or commercial agreements, the user could be asked for download approval. User approval may not be necessary for all downloads. The requirement means that a mechanism to ask the user is available but it may be used or not depending on the specific download.

Download_Suspend:

In the case of OTA (Over-The-Air) upgrade, the download should resume if interrupted. Indeed, the download of the new radio interface or protocol stack is process which can be interrupted either by the user (if he switches off his equipment) or by an external event (loss of the radio link, weak battery...).

Obviously, the new software cannot be installed. However, it can be useful to resume the download (not from scratch but from the state just before the interruption).

This requirement can be useful:

- To minimize the overhead in the radio access network,
- To minimize the lost time when the user cannot receive/send communication with his phone due to the fact that his equipment cannot support the new radio interface.

Download_Stop:

In case the user change of needs or the process failed or the process can not be suspended. In this case, the download process cannot be resumed.

3.3.6 Reconfiguration Management

Capability: Reconfiguration Management (ReconfigurationMgmt)

The end-to-end reconfiguration control management actions are assumed to be carried out by a Reconfiguration Manager. The reconfiguration process might be initiated either by the user equipment or by the network.

Requirement identification: **ReconfigurationMgmt_Dynamic**

The reconfiguration of protocol stacks supporting a mode of operation SHALL be performed dynamically: without shutting down the processor or the operating system.

Requirement identification: **ReconfigurationMgmt_Transparent**

Reconfiguration execution SHOULD be transparent to the user.

Requirement identification: **ReconfigurationMgmt_NoDisruption**

Reconfiguration SHALL be performed without any loss of information and without user perceived disruption.



Requirement identification: **ReconfigurationMgmt_Initiate**

Both equipment and network SHALL be able to initiate a reconfiguration.

Requirement identification: **ReconfigurationMgmt_Personalized**

The reconfiguration process SHALL be coherent with the various profiles' equipment/network/user/....

Requirement identification: **ReconfigurationMgmt_Atomic**

The reconfiguration process SHALL be executed in atomic steps

Requirements explanation

ReconfigurationMgmt_Transparent:

Once the reconfiguration process has started, it does not require any user intervention.

ReconfigurationMgmt_Initiate:

Both possibilities have to be provided by the implemented framework.

3.3.7 Service Adaptation

Capability: Service Adaptation (ServAdapt)

Active services can be adapted to changes in the network status (e.g. congestion) or modifications of the equipment (e.g. reconfiguration), or alteration of the access network used by a equipment (e.g. vertical handover). Service adaptation may cause reconfiguration in equipment in an attempt to avoid major disruption on the executed service.

Requirement identification: **ServAdapt_Dynamic**

Services SHOULD be dynamically adapted when a change in the system status occurs.

Requirement identification: **ServAdapt_Context**

Service adaptation MAY be context-driven: the service MAY trigger certain adaptation actions exploiting context information.

Requirement identification: **ServAdapt_Provide**

Based on the adaptation actions declared at its registration, context information modification and system status change SHOULD be transmitted to the Service Provider, in order to enable dynamical adaptation of the service.

Requirement identification: **ServAdapt_Continuity**

Service adaptation SHOULD be carried out with the service continuity ensured.

Requirement identification: **ServAdapt_MultCommLinks**

The equipment SHOULD be able to establish simultaneously multiple communication links using different radio access technologies in order to access one or multiple services.

Requirements explanation

Dynamic Service adaptation is enabled based on the potential adaptation actions declared at each value added service registration to a service aggregator/service provision platform or a mobile operator and the contextual information regarding the user and equipment capabilities and preferences. Such information is maintained by a context manager. A context manager should provide Reconfiguration Manager with such contextual information for the adaptation decision making.



3.3.8 Vertical Handover

Contextual information stands for semantic data. For example user context may be retrieved by specific sensors such as locator estimators, profile tagged values and charging issues. The retrieved information is semantically interrelated by such sensors so as to be obtained by any context manager. Information about these relations is described by contextual information, forming a meta-data level. So, in this example, user contextual location constraints the user preferences as referred in user profile and any registered user-oriented service adapts appropriately itself. Any context profile consists of certain and strictly reconfiguration oriented parameters. User and equipment profile extend the aforementioned context profile which their various parameters are specifically oriented to user and equipment mobile computing entities respectively.

Capability: Vertical Handover (VHO)

Equipments are able to move through different access networks without losing their active connections. VHO can be equipment or network initiated.

Requirement identification: VHO_Seamless

There SHALL exist mechanisms that enable the transfer of the context of the application/service for the seamless operation of 3rd party applications/services when performing a vertical HO between different NOs.

Requirement identification: VHO_RealTime

The handover process SHALL be completed in real time without delays that may cause service interruption. Additionally, the packet loss must be minimized. To accomplish this, different handover algorithms may be available to be downloaded and executed.

Requirement identification: VHO_Personalized

Handover decision SHOULD be based on contextual information (user/paying capabilities, user/QoS demands, system capabilities, system load) so that a compromise could be found among the various profile parameters.

Requirements explanation

Vertical handover can take place between the RATs of the same operator or between RATs of different operators. In the second case for the service continuity to be ensured there must exist mechanisms that allows the operators to exchange the context of the application or service. The transfer of services between cooperative RATs during the reconfiguration process must be seamless to the user.

3.3.9 Service Provision

Capability: Service Provision (SrvProv)

Service provision refers to basic telecommunication services as well as value added services offered by operators or independent VAPSSs.

Requirement identification: SrvProv_Open

Open APIs SHOULD exist for third trusted parties to register and make their software/services available to the users.

Requirement identification: SrvProv_Personalize

Service discovery SHOULD take into account on the user and equipment profile.

Requirement identification: SrvProv_NetCapability



A mechanism SHOULD be provided to the Service enabling to know the capabilities of the available access networks.

Requirement identification: **SrvProv_Custom**

Services SHOULD automatically customize according to the capabilities of the available access networks.

Requirement identification: **SrvProv_OneBill**

As much as possible billing information for the services used by a user SHOULD be incorporated in one single bill per service.

Requirements explanation

SrvProv_Custom:

This requirement is connected with reconfigurability as it is strongly related to what is called a Network Profile. Most probably the Network Profile will have to be defined/described from scratch: Network Profile collects static and dynamic information relevant to the capabilities and the resources of the network.

3.3.10 System Monitoring

The resources are the total means available to a network operator for switching, routing and handling the traffic associated with the services offered to users... This includes both tangible assets such as network infrastructure (base stations, antennas, etc.) and intangible assets (such as spectrum).

Capability: System Monitoring (SysMonitoring)

The equipment and network SHALL be able to monitor the current state of system operation (traffic, used spectrum, available technologies) in order to be able to estimate available resources and to facilitate the 'optimum' use of existing and available resources. The 'optimum' use of existing resources is a complex decision that has to take into consideration the interests of all the parties involved (user, operator, service provider...).

Requirement identification: **SysMonitoring_Detect**

The equipment and network SHOULD be able to detect variations in the operating conditions and act in order to make the best use of resources.

Requirement identification: **SysMonitoring_AltTechDetect**

The equipment and network SHOULD be able to detect the presence of other radio access technologies in a certain area.

3.3.11 Dynamic Resource Management

Capability: Dynamic Resource Management (DynResMgmt)

The network operator is able to dynamically assign its resources to the different tasks to be performed in order to make the best use of them.

Requirement identification: **DynResMgmt_Processing**

The network SHOULD be able to dynamically assign more processing resources to the different radio access technologies it offers to users.

Requirement identification: **DynResMgmt_Spectrum**



The network SHOULD be able to allocate its spectrum dynamically between the different radio access technologies it offers to users.

Requirement identification: **DynResMgmt_ServiceContinuity**

The operation of services by the users SHOULD not be interrupted nor affected because of the dynamic resource management process performed by the network.

Requirement identification: **DynResMgmt_EquipmentReconf**

It SHALL be possible for the network to ask a equipment to reconfigure to a different radio access technology or frequency.

3.3.12 *Spectrum Transfer*

Capability: **Spectrum Transfer (SpectrumTransf)**

The owners of the spectrum are able to transfer their spectrum to other parties through commercial agreements such as a re-sale or a lease. Besides, in order to make new spectrum available, move an existing technology to a different band or change the technology currently assigned to a certain band the regulator may decide to perform a reallocation of the spectrum assigned to communication systems.

Requirement identification: **SpectrumTransf_RightsRulesDef**

There SHOULD exist clear rules detailing the rights of the spectrum owner and the rules that it must follow for its operation and transfer.

Requirement identification: **SpectrumTransf_Respon**

In case of a temporal spectrum transfer (such as a lease) it SHOULD be clearly established who is responsible for its proper use.

Requirement identification: **SpectrumTransf_Parameters**

The parameters that specify the spectrum transfer (such as amount of spectrum, duration of the transfer or payment) SHOULD be clearly stated, logged and tracked.

Requirement identification: **SpectrumTransf_RegApprove**

A mechanism SHOULD be provided enabling the approval of Regulatory body before the spectrum transfer can take place.

Requirement identification: **SpectrumTransf_EqOpp**

In case of new spectrum allocation the regulator SHOULD ensure that all the entities allowed to use it have equal chances to access it.

Requirements explanation

These requirements establish some rules that should be followed if spectrum transfer between parties is allowed. If spectrum transfer is not possible or allowed then these requirements do not apply.

SpectrumTransf_Respon:

Requirement explanation: Two different possibilities in this case are that either the owner of the spectrum is responsible for its correct use (even though the spectrum use has been transferred to another party), or the party that acquires the spectrum is responsible for its proper use (though it is not the owner of it).

SpectrumTransf_RegApprove:

Such mechanism should be once and off-line approved by a Regulatory body. Every individual case of spectrum transfer will be based on certain and possibly ad hoc commercial agreements



Wireless World Research Forum
Working Group 6 White Paper
*Scenarios, system requirements and roadmaps for
reconfigurability*



between mobile operators, whilst it will be carried out based on the approved mechanism. Such mechanism may be a part of the aforementioned commercial agreement.

3.4 Conclusions

After deep analysis of the scenarios, requirements have been captured and organized in capabilities. The list of requirement constitutes the specification of the reconfigurability framework that has to be elaborated. The various requirements are intended to be satisfied by functions distributed on the various elements constituting the system. Some of the requirements may be today orthogonal depending of the context of application. The requirements list can not be considered as definitive at this stage of the project definition. During further analysis of the design, technological constraints and architecture elaboration will have impact on the requirements list.



4 ROADMAPS FOR RECONFIGURABILITY

4.1 Introductory approach

The scope of this section is to expose Business Models regarding the technological roadmap and to propose a Business path coherent with the technology evolution which will support the evolution towards reconfigurability for each identified actor of the value chain. In addition, in this section we attempt to trace a plausible roadmap for the deployment of reconfiguration applications into equipment and by extension into networks. Such a roadmap may serve as a guide in anticipating evolution, identifying important problem areas and if possible contribute to appropriate organisations (e.g. standard bodies, international fora) in meaningful topics. A roadmap is needed in order to put technology into perspective and for handling the complexity of difficult problems by defining an evolution path of incremental technology introduction.

4.2 Business Models

Reconfigurability opens the possibility for third party software vendors to provide high-level as well as low level system software. It also allows different actors to trigger changes, like upgrades, to the HW/SW combination of the equipment, even after the equipment has entered the market. In such scenarios, the assignment of responsibility becomes quite crucial.

The settings and software combinations of equipment, already for non-reconfigurable technologies, are rather complex. The manufacturer installs the firmware, operating system and basic applications while the operator may include some tailored platform software and applications. All of these installations may be correct or they may have bugs which potentially require patching. While this, in recent terminals can be done, to a certain extend, rather easily, such patching will become rather problematic when system configuration software may be procured and installed even from/by third parties.

Much of the flexibility and the value that is added through reconfigurability are based on software download and controlled installation/ activation. This however relies on sufficiently secure mechanisms for download and trust into origin, download path, suitability and authenticity of the software.

For operators there are two main problem areas; in case reconfigurations cause any problems, the operator will be the main point of contact (and blame) for the user, thus failed reconfigurations can potentially harm the operators reputation. The second problem is in the efficiency of use of an operators' spectrum. Reconfigurations may lead to inefficiencies or misuses and consequently resulting in revenue loss. There may be many other potential problems, yet the shared theme of all problems identified is the need for a common scheme to assign the responsibilities for reconfiguration.

As aforementioned, there are many actors involved in reconfiguration procedures, and their interests and dealings may be rather complex; these actors, their tasks and their relations need to be identified and the roles they play in reconfiguration processes needs to be evaluated.

A distinction of two dimensions in which actors may operate can be made: the first being the operational and the second the administrative dimension. We could identify fifteen actors have been identified for end-to-end reconfigurable systems: User, subscriber, network operator, equipment manufacturer, (value-added) service provider, content provider, software provider, service aggregator, regulator, reconfigurable equipment, reconfiguration manager, certification entity, security entity, pilot channel provider and spectrum manager.

Focusing on some of these actors, their roles in the operational dimension include:

Equipment Manufacturer

Provides the reconfigurable platform, firmware and software updates/new versions.

Network Operator

Owns the spectrum as well as the infrastructure, can also act as service provider

Software Provider

Third party providing application software, but also low level configuration relevant software

Service Provider

Provides the required/requested services, this may also imply the possibility that an end user may act as service provider

Reconfiguration Support Service Provider (e.g. Reconfiguration Manager)

Provides the basic services necessary for reconfiguration, including for example secure software download

User/Subscriber

Uses the equipment and infrastructure, may request installation of new configuration of application software.

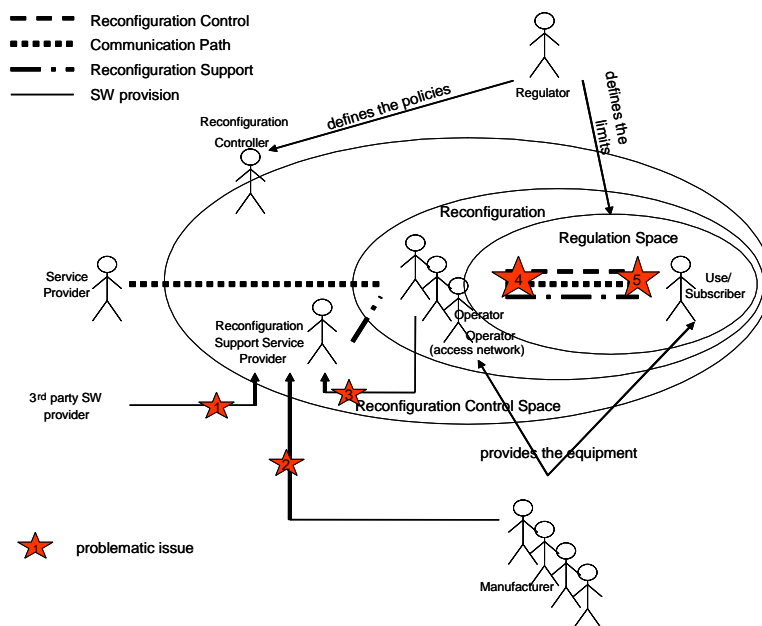


Figure 4: Actors in End-to-End reconfigurable Systems



While in the administrative dimension, the same actors may assume different roles:

Regulator

Sets the framework for use of reconfigurable equipment, allocates the spectrum to lease holders and governs (using policies) the usage of the spectrum and the circulation of reconfigurable equipment.

Reconfiguration Controller (e.g. Certification Entity, Security Entity, Spectrum Manager)

Verifies that intended reconfigurations will comply with given standard or that the equipment is prevented from implementing an intended configuration. This controller also implements functions like spectrum management according to given policies and certifies the intended configurations of the reconfigurable equipment,

Equipment Manufacturer

Arranges and initiates (performs) software (firmware) updates and patch installation,

Software Provider

Provides third party system, protocol and application software,

Service Provider

May request the reconfiguration of equipments to enable the provision of its services,

Reconfiguration Support Service Provider (e.g. Reconfiguration Manager):

Provides the control and security features for the reconfiguration procedure, independent of who may have initiated the reconfiguration process,

Network Operator

Provides the radio resources, mobility management and fixed capabilities to switch, route and handle the traffic associated with the services offered to users,

User/Subscriber

May initiate, allow or decline a reconfiguration.

4.3 The Responsibility Chain Concept

This subsection looks into a complete end-to-end reconfigurable system, focusing on the administrative roles of the various actors involved (see figure 1). The figure outlines, in the context of the end-to end-system, the main points of where actors (and their activities) may interfere with the system functions and where they will have to take responsibility for the system state.

There are a number of rather sensitive areas (indicated by the stars in the figure) that may be affected during a reconfiguration procedure.

Issue 1 highlights the question of the actor who takes the responsibility for third party software and who vouches that such software can be used to implement a radio protocol on the platform built by a specific manufacturer.

Issues 2 and Issue 3 tackle the same situation but in these cases the software would be provided by the equipment manufacturer or operator, respectively, and the configurations would be used in a different administrative domain.

Issue 4 tackles the matter about permitting (reconfigured) terminals to access/use an operator's Radio Access Technology (RAT).



Wireless World Research Forum
Working Group 6 White Paper
*Scenarios, system requirements and roadmaps for
reconfigurability*



Issue 5 deals with the problem of who can (and will) take the responsibility if a terminal is being reconfigured.

Issues 4 and 5 include the prevention of misuse of spectrum (e.g. in the Cognitive Radio Approach, when a user does not release the spectrum) as well as the spectrum control.

To approach these problems, the relationships between the actors in end-to-end reconfigurable environment have to be defined and established.

The responsibility chain concept provides an initial overview of the different responsibilities and aims to do this definition of these relationships. The chain needs also be connected to the value chain of mobile telecoms, with the aim to outline possible sanctions if the assigned responsibilities are violated. The responsibility chain defines a model where the accountability for reconfigurations can be assigned to the different actors within end-to-end reconfigurable systems. Connected to the concept of value chain in the definition of the business models for end-to-end reconfigurable systems, the responsibility chain will need to identify the dynamic interactions between actors encompassing information data, control data and money flow and will need to define a penalty scheme to penalize violations or infringements with actors rights as result of reconfiguration procedures.

4.4 Reconfigurability Roadmaps

The roadmaps treat two popular use-case scenarios. First comes the scenario for over-the-air (OTA) software upgrades and second comes the scenario for dynamic radio mode and standard switching. These two scenarios correspond to applications of reconfiguration that appeal to operators according to previous market studies on SDR. Figure 5 graphically depicts the deployment roadmaps separately for each scenario.

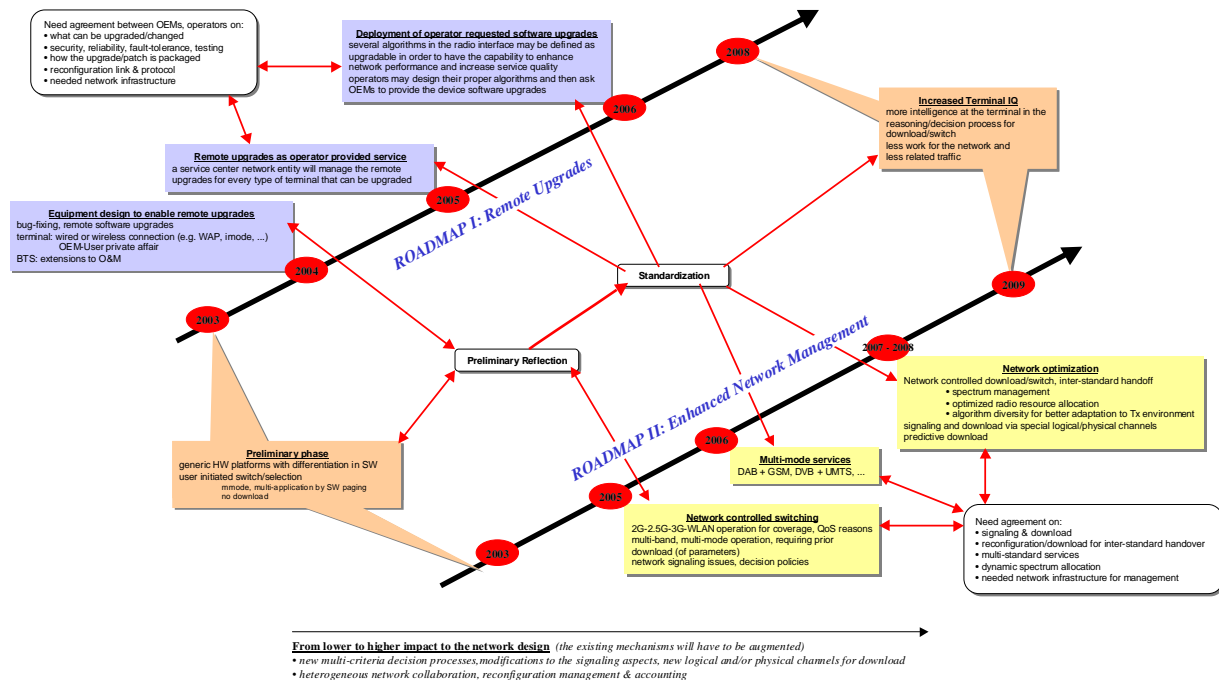


Figure 5: Deployment Roadmaps for Incremental Introduction of Reconfigurability Applications

Over the past ten years previous work on SDR has set a solid foundation for the future evolutions represented by these two roadmaps. Technical issues have been investigated in depth by the SDR Forum. SDRF provided feedback to 3GPP in order for MExE to make provision for the software download required by reconfigurable radios. In this spirit the *introductory phase* indicated in the roadmaps is based on this previous work. Further work in state-of-the-art survey will help to better identify the current status.

The *introductory phase* consists in designing the devices in such a way that part or all of their radio functionality is designed to be modifiable by means of software change. This requires from one hand using generic hardware platforms and increasingly software implementations and from the other hand a software architecture permitting to completely or partially modify its function statically or dynamically. In addition, at the network side there is provision in the standards (e.g. 3GPP TS 22.129) for 2G to 3G seamless handoff (i.e. GSM to UMTS). This currently works under the assumptions that standard switching does not need download and that core networks are compatible.

After this introductory phase the technical focus will shift from the radio implementation to the reconfiguration aspects of SDR as well as the network involvement in the reconfiguration process. To handle these aspects previous research work, like for instance results of EU projects, provides a good starting point. Within previous studies in 5th IST FW programme dedicated studies have been performed about downloading and SDR mechanisms for dynamic installation and test on new SW modules in a terminal. Several projects (TRUST, CAST, PASTORAL) contributed to elaborate proposal for implementation of Reconfiguration control unit able to access and reconfigure SW modules at each layer of the system (Application, Protocol, physical



Wireless World Research Forum
Working Group 6 White Paper
*Scenarios, system requirements and roadmaps for
reconfigurability*



layer) These results allow to anticipate that the concept can be implemented into wireless/mobile terminals, the main limitations are linked to cost, consumption and targeted features that have to be defined for these future systems.

Past experience shows that technologies evolve from simple towards more complex applications and on a need basis. Thanks to its simplicity, the scenario on software upgrades for bug-fixing and for performance enhancement as well as algorithm dynamic change (i.e. algorithm diversity) within a single mode of operation could be deployed first. Next will come simple robust schemes (e.g. based on parameter controlled reconfiguration for multi-mode/multi-service operation without or with minimal network implication. These schemes will eventually permit download and reconfiguration signalling through logical/physical channels existing within the mode of operation (e.g. GSM logical channels or GSM based wireless internet links). Alternative uplink air-interfaces could be used whenever the mode of operation disposes only of a downlink, (e.g. DAB/DVB). During this period device reconfiguration mechanisms and designs will mature a high degree of reliability of the reconfiguration processes will be attained and regulation issues will be more clear. At the same time moving towards 4G will advance work on network interoperability and network management unification. This fact will push forward software radio applications requiring more network involvement and cooperation. An all-IP approach will certainly facilitate resolving these interoperability issues. Such application may target things like:

- Dynamic spectrum and network resource management,
- More intelligent air-interface selection for "best" communication and service integration.
- Flexible service discovery and provision
- Reconfigurable applications to support context aware network wide reconfigurability
- Reconfigurable charging and security schemes

Finally, progress in the domain of identification algorithms will greatly contribute in making the reconfigurable radio devices increasingly independent.

As it is shown in Figure 5, in all cases there is need for standardisation. Standards will define the required device capabilities, the needed network infrastructure support as well as the communication links and protocols needed for signalling and data transfers. As a conclusion it can be said that the way reconfiguration capabilities will be deployed in the future is not yet completely known.

The above roadmaps are only a plausible work hypothesis and have to be taken as such. Other interesting use-case scenarios most probably will have to be considered as well. Commercial applications will initially consider existing air-interfaces. This is because work on future air-interfaces (e.g. 4G) is still ongoing. However a reconfigurable SDR approach offers the benefit of making possible future transition with a low impact on existing infrastructure.

As the deployment will be incremental; in between deployment phases experimentation is certainly needed. System prototyping will be a valuable approach in order to concretely demonstrate solutions into a smaller scale before their application in a larger scale. Such experimentation and prototyping could be part of R&D projects investigating future telecom systems.



Wireless World Research Forum
Working Group 6 White Paper
Scenarios, system requirements and roadmaps for
reconfigurability





5 CONCLUSIONS

Recapitulating, this paper started with a presentation of some typical scenarios envisaged to occur in a reconfigurability context, outlining specific facets of reconfigurability. According to these scenarios, the basic requirements were extracted, with respect to a whole system capable of supporting reconfigurability. In addition, the commercial success of reconfigurable systems was considered and the respective roadmaps to this success.

In conclusion, the remarkable increase in the utilization of telecommunication services has been expressed through the continuous influx and use of revolutionary applications. This unstoppable evolution of telecommunications is expected to be facilitated by the key concept of next generation's wireless systems, namely the reconfigurability concept.

The worldwide research frameworks currently consider the requirements that need to be met in order to enable terminals and network elements to adapt transparently, securely and efficiently to specific conditions, e.g. hot-spots. In addition, it is anticipated that reconfigurability will bring advantages for all the actors of the wireless world. Roaming capabilities and applications will be offered to users, network providers will acquire more options for achieving the required QoS and capacity levels, through their infrastructure and for introducing value-added services more easily. In addition, manufacturers and service providers will benefit from the flexibility offered, in order to evolve their devices and services respectively.

Consequently, special attention must be placed upon reconfigurability, in order to provide the prerequisites for the commercial vitality of newly developed wireless infrastructures and influence positively users in using innovative applications.



6 REFERENCES

- [i] M. Mouly, M.-B. Pautet, "The GSM system for mobile communications", published by the authors, Palaiseau, France, 1992
- [ii] R. Kalden, I. Meirick, M. Meyer, "Wireless Internet access based on GPRS", IEEE Personal Commun., Vol. 7 No. 2, April 2000
- [iii] 3rd Generation Partnership Project (3GPP) Web Site, www.3gpp.org
- [iv] Institute of Electrical and Electronics Engineers (IEEE) 802 standards, Web site, www.ieee802.org, 2004
- [v] J.Khun-Jush, P.Schramm, G.Malmgren, J.Torsner, "HiperLAN2: Broadband wireless communications at 5 GHz", IEEE Commun. Mag., Vol. 40, No. 6, June 2002
- [vi] U.Varshney, "The status and future of 802.11-based WLANs", IEEE Computer, Vol. 36, No. 6, June 2003
- [vii] Digital Video Broadcasting (DVB) Web site, www.dvb.org, Jan. 2002
- [viii] P.Demestichas, L.Papadopoulou, V.Stavroulaki, M.Theologou, G.Vivier, G.Martinez, F.Galliano, "Wireless beyond 3G: Managing Services and Network Resources", IEEE Computer, Vol. 35, No. 8, Aug. 2002
- [ix] D.Kouis, P.Demestichas, V.Stavroulaki, G.Koundourakis, N.Koutsouris, L.Papadopoulou, N.Mitrou, "A system for enhanced network management towards jointly exploiting WLANs and other wireless network infrastructures", accepted for publication in the IEE Proceedings in Communications Journal
- [x] End to End Reconfigurability (E2R), IST-2003-507995 E2R, <http://www.e2r.motlabs.com>
- [xi] P. Demestichas, N. Koutsouris, G. Koundourakis, K. Tsagkaris, A. Oikonomou, V. Stavroulaki, L. Papadopoulou, M. Theologou, G. Vivier, K.El-Khazen, "Management of networks and services in a composite radio context", IEEE Wireless Commun. Mag., Vol. 10, No. 4, Aug. 2003, pp. 44-51
- [xii] P. Demestichas, V. Stavroulaki, "Issues in introducing resource brokerage functionality in B3G, composite radio, environments", IEEE Wireless Communications Magazine, Vol. 11, No. 10, October 2004
- [xiii] P. Demestichas, G. Vivier, K.El-Khazen, M. Theologou, "Evolution in wireless systems management concepts: from composite radio to reconfigurability", IEEE Communications Magazine, Vol. 42, No. 5, pp. 90-98, May 2004
- [xiv] P.Demestichas, V.Stavroulaki, L.Papadopoulou, A.Vasilakos, M.Theologou, "Service configuration and distribution in composite radio environments", IEEE Transactions on Systems, Man and Cybernetics Journal, vol. 33, No. 4, pp. 69-81, Nov. 2003,
- [xv] Software Defined Radio forum: www.sdrforum.org
- [xvi] IST project SCOUT (Smart user-centric communications environment), www.ist-scout.org
- [xvii] Paul Leaves, David Grandblaise, Ralf Tönjes, Klaus Moessner, Michele Breveglieri, Didier Bourse, Rahim Tafazolli, "Dynamic Spectrum Allocation in Composite Reconfigurable Wireless Networks", IEEE Communications Magazine, Vol. 42, No. 5, May 2004



1 APPENDIX : CONTRIBUTING AUTHORS

Panagiotis Demestichas pdemest@unipi.gr

Flora Malamateniou flora@unipi.gr

G.Kritikou, kritikou@unipi.gr

George Dimitrakopoulos gdimitra@unipi.gr

Didier Bourse Didier.bourse@motorola.com

Karim El Khazen karim@motorola.com,

Stephen Hope Stephen.hope@orange.co.uk

Makis Stamatelatos g.stamatelatos@di.uoa.gr

Nancy Alonistioti nancy@di.uoa.gr

Alexandros Kaloxylos agk@di.uoa.gr

Kostas Kafounis kafounis@di.uoa.gr

Panagis Magdalinos p.magdalinos@di.uoa.gr

Enrico Buracchini enrico.buracchini@tilab.com

Paolo goria paolo.goria@tilab.com

Alessandro Trogolo alessandro.trogolo@tilab.com

Guillaume vivier Guillaume.Vivier@crm.mot.com

Antoine Delautre antoine.delautre@fr.thalesgroup.com

Miguel Alvarez macalvo@tid.es

Raquel Garzia rgp@tid.es

Francois Marx francois.marx@francetelecom.com

Georges De Brito georges.debrito@francetelecom.com

Marylin Arndt marylin.arndt@francetelecom.com