SOME IMPORTANT ASPECTS OF RECONFIGURABLE SOFTWARE RADIO DESIGN

Asok Bandyopadhyay, *Joint Director, C-DAC, Kolkata*
Plot E2/1,Sector V, Block GP, Salt Lake, Kolkata-700 091
e-mail: asok.bandyopadhyay@cdackolkata.com

ABSTARCT

This paper reflects the issues related to the reconfigurability property that software radio needs to satisfy for implementing the software radio concept and corresponding trends in industry for reconfigurability. Even though current technology limits impose deviations from the ideal all-software- radio, the advent of high-density reconfigurable hardware (FPGAs) as well as proper system engineering and design, make the software radio concept a viable reality and the concept of Hardware/Software co-design becomes more relevant. Lastly, as reconfigurability and reconfiguration open up SWR systems to the outside world, issues like security, safety, reliability, become of extreme importance.

1.0 INTRODUCTION

In software radio most of the analog signal processing operations of the radio transmitter and receiver are implemented with digital hardware using DSP techniques; the receiver ADC and the transmitter DAC are placed closed to the antenna. In the software radio receiver, the approach often used is to digitize an entire band and to perform IF processing, base band, bit stream and other functions completely in software. However, the signal processing requirements for military and commercial radio systems employ high data rate signals or spread spectrum modulation, where special purpose DSP hardware, application specific devices and field programmable gate arrays can play an important role. Very high-speed front-end signal processing suits FPGAs, which can handle ultra-fast computation for complex filtering, mixing, and coding/decoding signal processing. Reconfigurability entails the pervasive use of software reconfiguration, empowering upgrades or patching of any element of the network and of the services and applications running on it.
Reconfiguration allows upgrading and adapting equipment to user preferences and local conditions. Besides the installation of bug fixes, it will be possible to adapt and upgrade communication protocols, codecs, base-band processing algorithms or the complete air-interface (software radio).

2.0 SOFTWARE RADIO

The term software radio was first coined by J. Mitola in [1]. In its ideal realization wideband signal digitization occurs next to the antenna and the rest of the radio processing is implemented in software running on a very fast general-purpose processor. This concept is depicted in Fig. 1.
Software radio is all about tailoring the concept of reprogrammability to the domain of radio communications so as to enable the use of generic hardware/radio platforms for different types of radio applications just by changing the software. However due to current technology constraints such as lack of wideband ideal A/D interface, limited processor speeds etc., alternative architectures need to be devised to describe the currently feasible precursors of the ideal software radio while waiting for the enabling technologies to catch up.

2.1Critical Functionalities of a Generic Software Radio Receiver

In order to determine which functionalities have to cope with the strongest constraints and which are to be

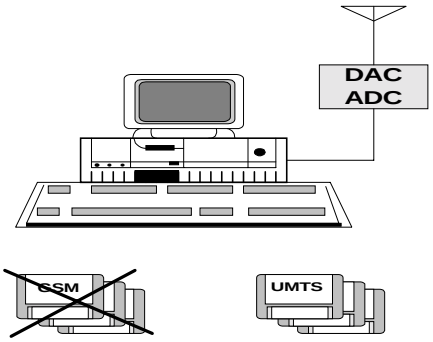

Fig. 1 Ideal SWR where all radio processing is in software

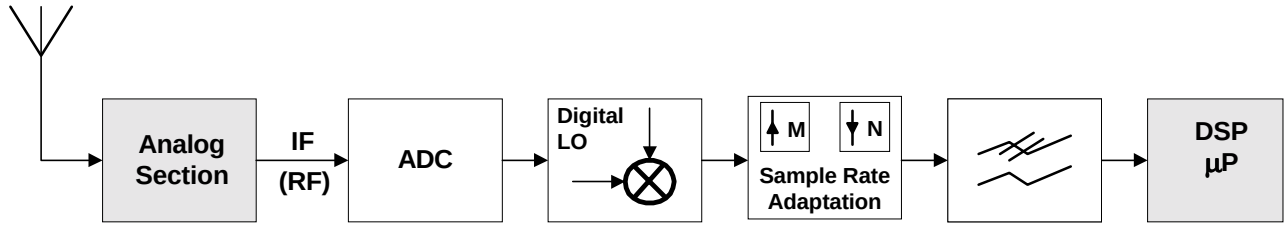

Fig.2 Generic Receiver for Software Radio Terminals

parameterizable or programmable, two basic design criteria that are sensible when trying to maximize simplicity are given (as shown in Fig.2) :

1) Analog components should be minimized and be fixed (non-parameterizable)
2) The system clock should be fixed, i.e. the ADC and the digital signal processing hardware is clocked with a (generally) constant rate.

The aim is to have as much adaptive functionality in the receiver as possible i.e. to perform IF- or even RF sampling. This leaves the antenna, the LNA, the system-filter, and in case of IF-sampling a down-converter to the analog domain. With regard to current technologies the effort in the analog domain has thus been minimized. The analog components are designed to fulfill the constraints of all services to be supported in the software radio receiver. High dynamic range in connection with relatively wide bandwidth makes the ADC as the critical component of every software radio receiver. If the signal cannot be transferred into a DSP there is no use of high-speed DSPs or sophisticated software. Thus the ADC is regarded as one of the so-called 'critical functionalities' [2].

2.2 Important Aspects of Digital Signal Processing Technique in SWR

The advantages of Software Radio are reached by the application of Digital Signal Processing techniques. On the digital signal processing side the critical functionalities are:

1. Digital Down-Conversion
2. Sample Rate Adaptation and Decimation, and
3. Channelization and Interferer Cancellation / De-spreading.

2.2.1 Digital Down-Conversion

Partial-Band Digitization of a signal at IF is selected as an appropriate means of digitization for software radio terminals. Since signal processing is almost always simpler and thus more efficiently performed at base-band the digitized signal has to be down-converted first. Digital down-conversion after analog-to-digital conversion has one main advantage compared to analog down-conversion before AD conversion: Perfect I-Q matching and thus image rejection can be realized.

2.2.2 Sample Rate Adaptation and Decimation

With these assumptions following approaches to sample rate adaptation can be named:

1.By keeping the ratio between IF and sample rate according to equation, $f_{IF} = n/4\ f_S$, n = 1,3,5, ... , where f_S is the sample rate Both, IF and sample rate, can be made parameterizable, so that each signal can be digitized with the clock rate of the standard of current operation, keeping the opportunity for simple down-conversion.

2.By digitizing with a fixed clock rate at a fixed IF digital sample rate adaptation can be performed by means of mathematical interpolation.

2.2.3 Channelization and De-Spreading

Channelization is the functionality where in FDMA systems the tasks of channel filtering (channel selection) and interferer cancellation are performed. This is dependent upon the previously described task of Sample Rate Adaptation and Decimation. Since decimation filters are low-pass filters they work as coarse channel selection and interference cancellation filters. Only fine, sharp cut-off filtering has to be realized 'alone'. De-Spreading is the functionality where in spread-spectrum systems the task of de-correlation and sample rate decimation to symbol rate is realized.

3.0 HW/SW CO-DESIGN FOR SOFTWARE RADIO

Due to the technology shortcomings in DSP speed, moving the digital processing closer to the antenna necessitates the introduction of specialized hardware processing in the form of ASICs and/or FPGAs, which offer higher reconfigurability. Furthermore, the coexistence of reconfigurable hardware (FPGAs) and microprocessing elements opens up the possibility to implement part of the functionality in software and another part in hardware. Thus, designing reconfigurable radio systems becomes simply an instance of the hardware/software co-design problem. Co-design is important due to the need to be able to rapidly develop the desired configuration for our flexible hardware engine and thus materialize the benefits from reconfigurability.

Finally, in the implementation phase the hardware, software and communications between processing elements are synthesized. The latter includes the hardware/software synthesis. Throughout the co-design process at each phase validation activities are employed in order to validate if the design objectives during a design phase have been met and decide whether to iterate or continue to the next phase. *Validation* techniques include simulation, formal verification, estimation, prototyping etc.

4.0 RECONFIGURABILITY

In the case of the ideal all-software-radio reconfigurability [3] is already built-in the system since DSPs or microprocessors can be reprogrammed just by changing the contents of their program memory.
From a software perspective, in order to be reconfigured, a terminal needs software module libraries that perform all the functionality for every protocol layer of a certain standard. The modules must be distinguished in accordance with their functionalities such as configuration modules, routines performing physical layer functions, and routines for supplying the services. Physical layer routine libraries consist of high-level object-oriented codes that perform any physical layer functions for the transmission standard supported by the terminal (e.g. modulation, demodulation, interleaving, equalization, source and channel coding and decoding, and so on).
This contribution concentrates on security requirements specific to the *reconfiguration* of communication equipment, where reconfiguration means that parameters or software in the device is changed. While some emphasis lies on the reconfiguration of the radio interface, reconfiguration can in general concern arbitrary parts of communication equipment as for example protocol stacks, plug-ins to support different types of content (as voice and video codecs), and applications. Main security issues are the control of the reconfiguration, that is who has the authority to reconfigure which parts of communication equipment, protection of the reconfiguration signaling, privacy of reconfiguration information as for example information on the current configuration of a user's equipment and of his preferences, the correctness and availability of information on which the reconfiguration is based, secure download of software required for reconfiguration, and issues concerning the radio emission and associated conformance requirements of radio equipment.

4.1 Reconfigurability and System Design

As it was previously mentioned current technological constraints make the ideal SWR impractical. Nevertheless, alternative architectures exist on which reconfigurable radios can be implemented. A high-level block diagram of such architecture is shown in Fig. 3.
At the receiver side we see an analog RF part that translates a wide input band of interest down to IF where the input analog signal is digitized using a wideband A/D interface. At this stage digital hardware takes us to the base band where additional digital hardware is in charge of the base band processing. The transmitter side takes the opposite direction. Additional external interfaces as well as the system control part are also represented. At the RF part there are analog circuits consisting of filters, amplifiers, mixers, etc.
Since this part is specific for each standard, it potentially limits the reconfigurability of the whole system. In this case the reconfiguration consists in a switch command that changes the hardware connections. The digital processing part is taken care by a mix of ASIC and DSP components. DSPs being reprogrammable they offer maximum reconfigurability. On the other hand the reconfigurability of ASICs depends on the number of operational parameters that can be set by software and usually their number is limited. For instance a digital modulator/demodulator can be configured for a limited number of modulation schemes. Filter components may further inhibit reconfigurability since different radio application may have quite different filtering requirements. Finally, connections between the various components

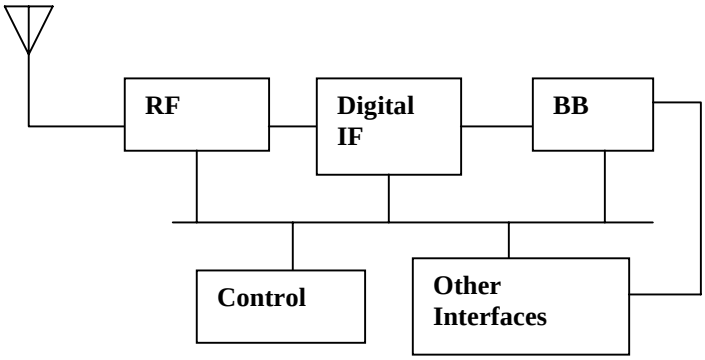

Fig. 3 Block diagram of reconfigurable radio architecture

cannot be rearranged at will since usually a limited number of bypasses are provided between individual system components. So, even though this architecture has a large digital part its reconfigurability has important limitations. However, the availability of high-density SRAM based FPGAs makes reconfigurability of the hardware functionality as high as that of software's. Features like fast reconfiguration times, partial reconfiguration and remote access to the FPGA resources, are also desirable [4] for SWR equipment. FPGAs have an important role to play in SWR in infrastructure base station equipment. It is important to understand that in order to effectively and seamlessly accommodate change; reconfigurability has to be designed in the system.

5.0 RECONFIGURATION SECURITY OBJECTIVES

Mobile communication systems using and supporting reconfigurable equipment require also security for aspects that are not specific to reconfiguration as for example protection of the air interface and controlled access to the network with mutual authentication of the user and the network, or protection of signaling traffic within and between operators.

5.1 Software Download

Dynamic software download is a key technology for reconfiguration. Malicious software could invalidate properties required for type approval or assured in a statement of conformance, but it could also lead to other types of harm. For example, it could circumvent other security mechanisms required for secure network access to a cellular network or a company's Intranet, or it could send a user's private data to unauthorized parties or make the device simply unusable. The device could also manipulate to behave against the user's interest, for example by calling premium rate services in the background, or by implementing a surveillance function (bug).
To prevent harm from potentially malicious software, two basic approaches Namely Sandbox Method and Trust-Based Method can be taken.

6.0 CONCLUSION

Reconfigurability and reconfiguration from one hand make possible to obtain the benefits from software radio implementations but from the other introduce a series of concerns relating to security, safety, reliability to name a few. Software radio systems become increasingly open to the outside world and thus increasingly vulnerable as well. As far as safety is concerned, think what may happen if a reconfigurable radio equipment is reconfigured to function in a way dangerous for its user. In terms of security questions like, -what if an unauthorized entity, uses reconfiguration in order to obtain confidential information about the user or the equipment itself, obtain unauthorized access to the network or break down the equipment-, are posed. Finally, reliability is summarized in the following question: what if an authorized reconfiguration makes the equipment unstable and its operation unreliable. In equipment with limited reconfigurability the ways that something can go wrong are also limited and users are accustomed to reliable operation. If such issues are not addressed adequately wireless equipment success will be compromised. Security has to be designed in the reconfiguration process. Reliability may also be achieved if reconfigurable radio systems are considered mission critical with fault tolerance techniques built in. Formal techniques in specification and verification have also interesting contributions when developing new configurations and for validating them before deployment.

7.0 REFERENCES

[1] J. Mitola, “*The Software Radio Architecture*”, IEEE Communications Magazine, vol. 33, pp. 26 - 38, May 1995
[2] Software Radio Receivers by Tim Hentschel and Gerhard Fettweis, Dresden University of Technology, Germany
[3] Reconfigurability: A Key Property in Software Radio Systems by Apostolos A. Kountouris Ph.D., Christophe Moy Ph.D., Luc Rambaud
[4] D. Nicklin, Xilinx, Electronics Engineering Magazine, *"Utilizing FPGAs in Re-configurable Basestations And Software Radios*".