White paper on SDR Technologies for the International Tactical Radio Market

Document WINNF-09-P-0006

Version V1.0.0

14 September 2011

TERMS, CONDITIONS & NOTICES

Table of Contents

List of Figures

List of Tables

Introduction

From the Project Approval Document:

The *White paper on SDR Technologies for the International Tactical Radio Market*

That *identifies the issues that need to be resolved to enable a successful market*

Unlike *reports from other organizations like Frost & Sullivan or Forecast International*

This product *provides issues on an international basis, not just programs like JTRS, from an international base of members that include customers, primes, contractors and suppliers.*

Scope

The goal of the study is to identify the main trends for tactical radios in light of modernization efforts underway in various regions and markets and in the perspective of future net-centric operations.

The study and report will not recommend solutions to the issues or trends. It is expected that these will be addressed with future work efforts.

Executive Summary

Even if the market for Software Defined Radios (SDR) is considered as growing, it is still maturing: there are still some key supporting technologies, specifications and market business models being either in development or still to be discussed to date.

This White Paper, after providing some overview of Software Defined Radio (SDR) technologies for Tactical Communications Systems, highlights some key issues to be further addressed to increase the adoption of SDR technology by the market:

- Improving the WF portability: issues associated with Application Programming Interface (API) development,
- SDR Standards Compliance Certification
- Safety Certification
- Security aspects

1 SDR Technologies for Tactical Communications

1.1 Introduction to Software Defined Radio (SDR)

The Wireless Innovation Forum has provided an overall description of the Software Defined Radio concepts. A number of definitions can be found to describe Software Defined Radio (SDR). The Wireless Innovation Forum, working in collaboration with the Institute of Electrical and Electronic Engineers (IEEE), has worked to establish a definition of SDR that provides consistency and a clear overview of the technology and its associated benefits.[1] Simply put Software Defined Radio is defined as[2] *"Radio in which some or all of the physical layer functions are software defined"*

Please refer to the "What is Software Defined Radio" document issued by the Forum on its Web site at address:

http://www.wirelessinnovation.org/page/What_is_SDR ,

to access to the following document:

http://data.memberclicks.com/site/sdf/SoftwareDefinedRadio.pdf

In particular, an SDR is radio equipment whose waveform modulation/demodulation functions (and higher layer functions including coding, link layer, Information Security, networking etc.) are completely defined in software and whose functions can be redefined by a new software download. SDR technology has been enabled by:

- Increased speed and power of embedded processors, DSPs, FPGAs
- Improved performance of analogue to digital converters, higher conversion rates and increased dynamic range
- Application of object based programming techniques and middleware, such as CORBA permitting hardware abstraction and independence
- Development of effective software architectures for deploying waveform applications across the heterogeneous processing architectures they necessarily contain

The military is interested in applying SDRs to military communications in order to enable enhanced interoperability, potential for incremental improvements to communications capability and reduced whole life costs of fielding communications capability.

This interest is mainly driven by:

- Common and open software architecture(s) that support product upgrades and technology insertion
- Reduction of legacy stovepipe radios specialized for specific waveforms with movement to multi-purpose, multi-role radios
- Reduced development costs due to the reuse of tactical radio applications (e.g., waveforms).
- Improved interoperability therefore reducing the number of types and quantities of fielded equipment and their associated maintenance

Enhanced Interoperability (National Joint services, NATO, Coalition Forces, joint Defense-Public Safety forces operations etc…) is provided because SDRs are capable of:

[1] http://www.wirelessinnovation.org/page/What_is_SDR
[2] http://www.sdrforum.org/pages/documentLibrary/documents/SDRF-06-R-0011-V1_0_0.pdf

- Multi-roles (multi-waveform, multi-channel)
- Multi-bands
- Multi-algorithm secure communications (programmable INFOSEC)

2 SDR Military Market Adoption

The SDR market for Tactical Communications is gaining momentum and we can notice multiplication of SDR Programs on a worldwide basis.

The first and driving market for SDR technology for Tactical Communications has been the USA with the JTRS Program(s).

JTRS Program Web Site : http://www.public.navy.mil/jpeojtrs/Pages/Welcome.aspx

"Since its inception in early 1997, the Joint Tactical Radio System (JTRS) has evolved from a loosely associated group of radio replacement programs to an integrated effort to network multiple weapon system platforms and forward combat units where it matters most - at the last tactical mile. (...)

The ultimate goal is to produce a family of interoperable, modular, software-defined radios that operate as nodes in a network that provides secure wireless communication and networking services for mobile and fixed forces, consisting of U.S. Allies, joint and coalition partners, and in time, disaster response personnel. (...)

JTRS is developing and positioning products to meet stakeholder requirements by providing information sharing capabilities and interoperability to the warfighter, and enabling improved situational awareness and significant battlefield advantage through advanced Net-Centric Warfare. (...)

JTRS is not just a radio replacement program; it implements Joint Net-Centric Warfare vision at the Tactical Edge – critical for Irregular Warfare and High-end Asymmetric Threats. (...)[3] *"*

On the international market, we can distinguish several drivers for SDR Programs for tactical communications:

- Network Centric Operations Transition: introduction of High Data Rate services and full IP networking capabilities at the tactical edge together with introduction new C4ISR (Command, Control, Communication, Computer, Intelligence, Surveillance and Reconnaissance applications).

---

[3] JTRS JPEO Web Site

- National/regional SDR Programs: Programs aiming to define new generation tactical communications, looking to develop either radio platforms, Waveforms, with a national/regional sovereignty target.
- Emergence of Coalition Waveforms to improve interoperability at international level on the battlefield.

The worldwide map highlights this growing international market, beyond the US JTRS Program, including:

- North-America
  - Canada is launching some tactical communications programmes, for instance “Integrated Soldier System” that could use some SDR technologies.

- Europe
  - Launch of the ESSOR program in 2009, by 6 nations : France, Italy, Spain, Sweden, Finland and Poland,
  - New generation tactical communications systems and National SDR Programs in Sweden (GTRS Program), Germany (SVFuA Program), France (CONTACT Program), Italy
  - Other programs aiming to introduce some SDR capabilities together with NCO transition and new generation tactical communications systems: Switzerland, Netherlands, Denmark, Norway, etc…

- Middle-East, Asia, Pacific
  - Multiplication of SDR Programs: South-Korea (TICN and TMMR Programs), Japan, Singapore, UAE, India…

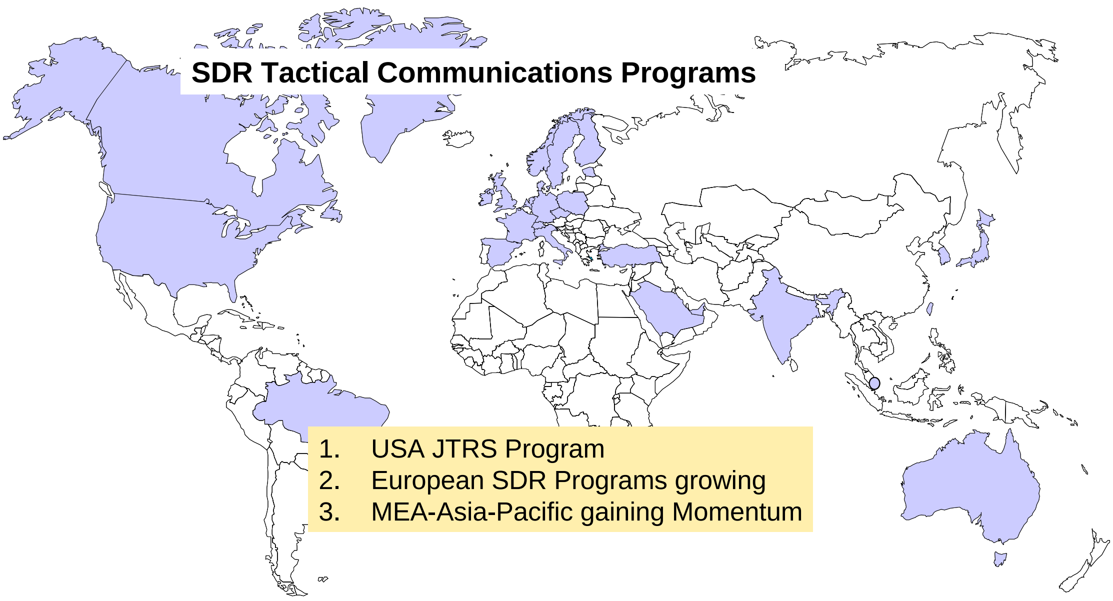

Figure 1: SDR Market Momentum

2.1 Interoperable Communications for Coalition Operations

One of the advantages of SDR is the ability to implement common or shared waveforms on tactical radios and for these radios to interoperate between nations for coalition missions.

Today, highly mobile forces, projected into remote theatres under joint or allied command, need to share a Common Operational Picture (COP), therefore pushing greater interoperability from application and IP level up to radio level, increasing connectivity between users on the ground, for joint and combined operations.

Enhanced interoperability among coalition partners is an essential requirement on the modern battlefield, with multinational coalitions becoming the norm for conducting military operations in hot spots around the world. Ongoing coalitions operations in Iraq, in Afghanistan, or in Libya, highlight this need for interoperability communications means on the battlefield and at the tactical edge.

The interoperability requirements are therefore part of all the recent and ongoing main SDR programs efforts.

2.1.1 JTRS Program

As highlighted in the main objectives, reported in the §3.2, "*The ultimate goal is to produce a family of interoperable, modular, software-defined radios that operate as nodes in a network that provides secure wireless communication and networking services for mobile and fixed forces, consisting of U.S. Allies, joint and coalition partners, and in time, disaster response personnel.'*"

2.1.2 US – UK Initiative: the JTRS Bowman WF

The US JPEO JTRS Program is leading a cooperative project between US and UK targeting interoperability on the field between US and UK units, using an SDR approach through the porting of the Bowman WF into US SDR JTRS architecture.

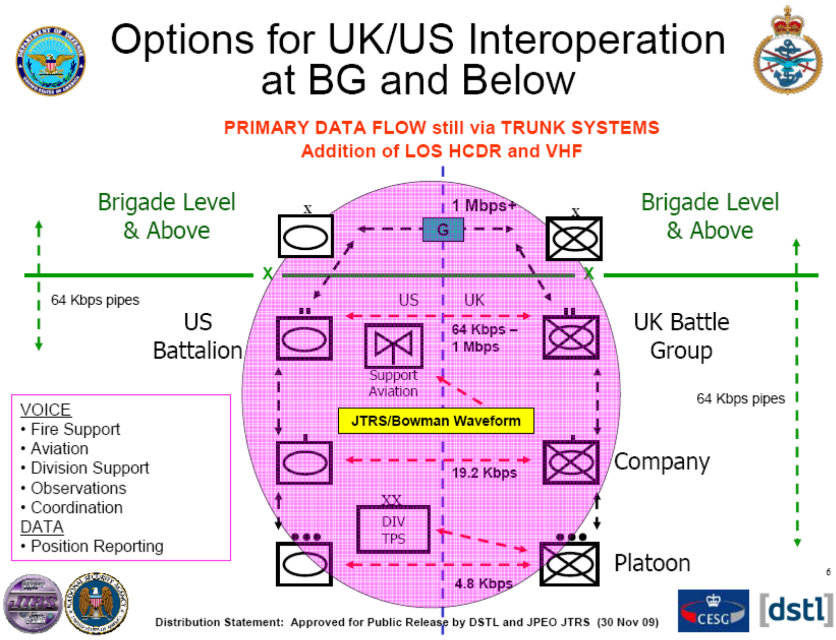

Figure 2 International Software Defined Radio 2010 Conference, London June 2010

Under the first phase of the collaborative programme, the UK Bowman VHF tactical waveform and associated crypto were developed and ported on to US SCA radio platform. The UK ADR+ VHF waveform (better known as JTRS Bowman waveform) is in the US JTRS Information Repository

Live network demonstrations have been performed in June 07 and Apr 09.

2.1.3 NATO Waveforms Working Groups

NATO has launched some initiatives to provide some wireless interoperability solutions for the battlefield, through some Working Groups (WG).

One WG aims at completing the development of the NATO Coalition Tactical Radio Waveform (CTRW), termed Narrow Band Waveform (NBWF). Work is ongoing between NATO and Industry to define and agree on common waveform standard (a RFI has been published in January 2011[4] to define the next steps).

As well, NATO has defined an SDR WF development framework.

[4] CRC Presentation – Tactical Communications 2011 Conference – London, April 2011

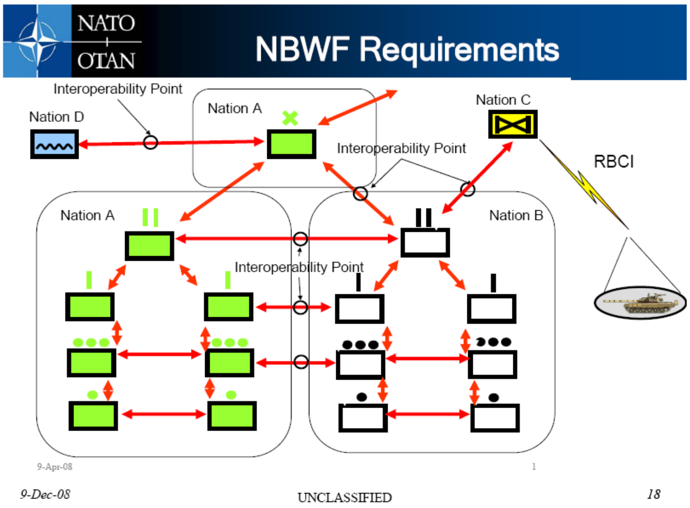

Figure 3 NATO – Ensuring Multinational Interoperability for Future Forces

2.1.4 ESSOR HDR Waveform

ESSOR: European Secure Software defined Radio

The main scope of this project is to provide architecture of Software Defined Radio (SDR) for military purposes and a military High Data Rate Waveform (HDR WF) to be used in coalition environment and compliant with such architecture, thus offering the normative referential required for development and production of software radios in Europe.

In addition, the project will deliver guidelines which are related to the validation and verification of waveform portability and platform re-configurability, setting up a common security basis to increase interoperability between European Forces.

The HDR Waveform is an Ad-Hoc HDR networking Waveform as highlighted in the following figure.

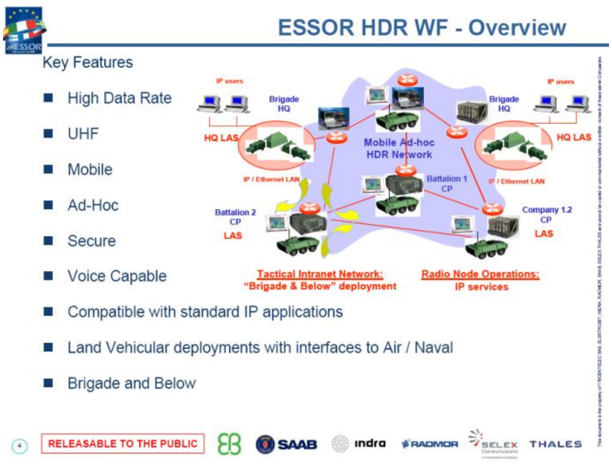

Figure 4 ESSOR HDR WF Overview

The ESSOR Architecture is a Software Defined Radio (SDR) Architecture building on the already published Joint Tactical Radio System (JTRS) Software Communications Architecture (SCA) and Application Programming Interfaces (APIs). The ESSOR Architecture is a complete and consistent Secure SDR Architecture addressing the European military radio-communications market, and fostering on Waveform portability amongst heterogeneous SDR Platforms.

2.1.5 COALWNW Program

In June 2009, nine nations (Australia, Finland, France, Germany, Italy, Spain, Sweden, United Kingdom and United States) agreed to jointly develop a wideband networking waveform to pass secure voice, video and data and to enable tactical interoperability among coalition forces. This waveform is known as the Coalition Wideband Networking Waveform, or COALWNW [5].

The COALWNW capability will be designed, developed, and tested using a three phased approach: (1) waveform specification, (2) waveform development (to develop waveforms to port to national radios), and (3) interoperability testing (Port COALWNW and conduct interoperability testing between national radios).

[5] UK DSTL Press Release – 9 Feb 2011 and France DGA Informations SDR Europe 2009 Conference

2.2 Benefits of Software Defined Radios for Tactical Communications

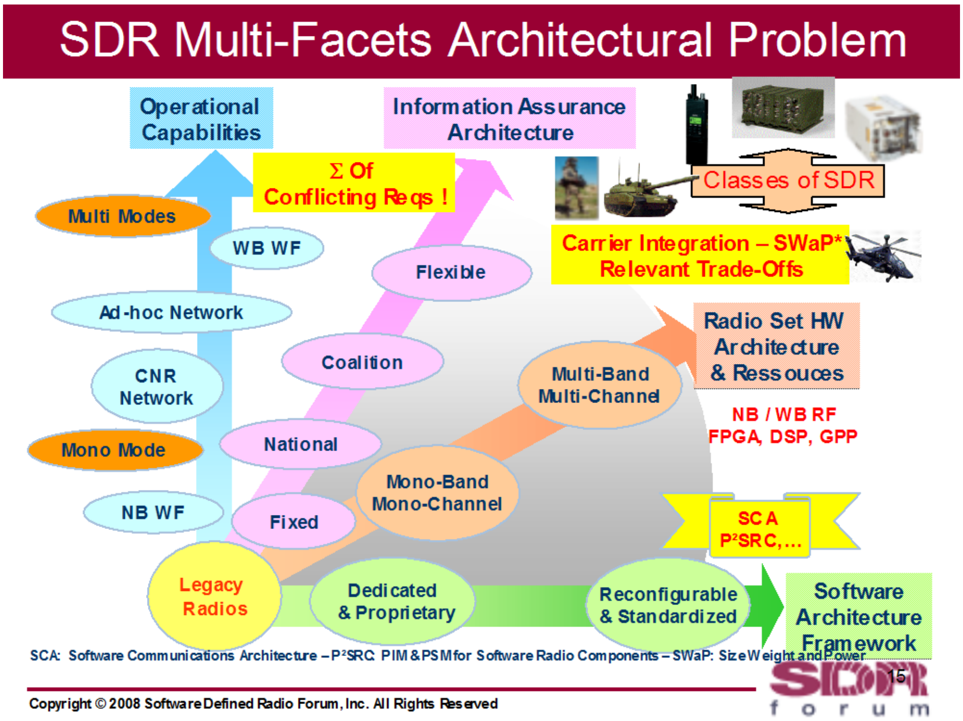

Figure 5 Wireless Innovation Forum – SDR Europe 2008 Conference, London, Dec 2008

The following are the key potential benefits that SDRs can offer:

- Multi-Band – The ability for a radio to be configured to work in a number of communications bands (e.g. HF, VHF, UHF, L Band) is key to supporting a wide range of new and emergent waveforms.
- Multi-Waveform – The ability for the same radio to work in a number of quite different operating modes (e.g. UK Bowman VHF, US SINCGARS, HAVEQUICK, Link 16).
- Multi-Channel – The ability to support multiple simultaneous communications channels. A multi-channel SDR may replace a number of discrete radios and, because of its multi-mode and multi-band capability, provide greater flexibility for the user.
- Upgrade Capability – Perhaps the single key benefit of SDRs, which differentiates them from previous technologies, is the ability to change their functionality in-service by installing/downloading a new or upgraded application (e.g. Operating Environments and Waveforms). New waveforms may include the actual signal-in-space (SIS), communications protocols, cryptographic (INFOSEC) algorithms and possibly network level applications including cross-banding/gateways etc. This allows new communications functions to be introduced in-service without, in many cases, making any changes to the installed equipment hardware. Such changes may

either be made using a direct fill, via a mission system fill or possibly (where applicable) via an over-the-air-rekeying (OTAR) type process.
- Interoperability Enabler - In-service capability enhancement provides great potential for enhancing future coalition/NATO interoperability because it breaks the old hard link between original equipment procurement defining a radio's capability and, in the case of SDR, its future capability through installation of new or upgraded interoperability waveforms.
- Size, Weight, Power Reductions – Since SDRs are capable of hosting many different waveforms, the need to have several special function radios, encryption devices etc is eliminated. Multi-mode, multi-channel SDRs have the potential to be very significantly smaller and lighter than the multiple legacy radios that they might replace (whilst also offering new capabilities).
- Whole Life Costs – It is believed that SDRs have the potential to significantly reduce the cost of providing communications capability by reducing the overall logistics costs of maintaining many different types of radio in service within a nation's Armed Forces.

2.3 Towards a Standardized SDR Architecture Framework

SDR equipment can be designed by radio manufacturers in a purely proprietary manner, as

- done in the commercial infrastructure wireless market,
- was done in the late 1990s for tactical communications for early SDR demonstrators (such as Speakeasy (US), FM3TR (US, UK, FR, GE), MMR-ADM (FR-GE)): these early SDRs demonstrated reconfigurability using different waveforms as well as interoperability with existing radios.

These early tactical communications systems demonstrated clearly to Procurement Agencies and Industry that a standardized SDR architecture framework could bring benefits in leveraging common waveform software development across a family of standardized SDRs, with the goal to foster interoperability and sharing of development costs amongst the interested parties, at national or multi-national levels.

This led to the development of the Software Communications Architecture (SCA) by US DoD as part of the JTRS program.

The SCA is a standard defining an Operating Environment (OE) that is embedded on the SDR platform and defines the standardized mechanisms to deploy and configure SDR waveforms on these platforms. In addition, the SCA defines a set of common APIs to be used by waveform applications running onto these SDRs with the goal of further standardizing the services offered by the SDR platform.

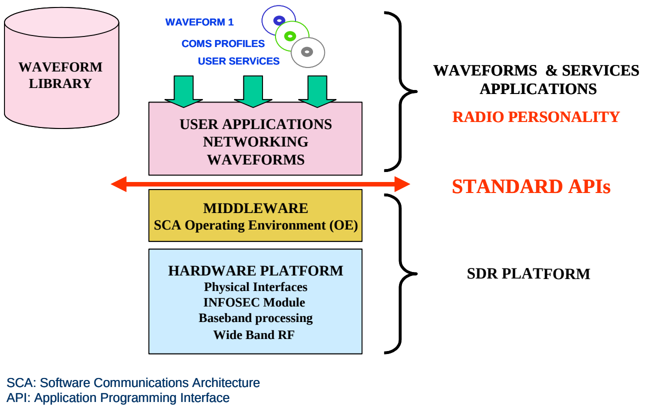

Figure 6 SCA: Software Communications Architecture

It should be noted however that the SCA does not address the standardization of hardware modules, leaving full and open competition for the development of the relevant SDR Platforms by industry. In fact, these industry players could develop/obtain their Operating Environment software from COTS vendors thereby lowering the cost impact of delivering such standardized SDRs.

Some new efforts to enhance the SDR Architecture are on going through the European ESSOR Program and the US JTRS SCA Next initiatives. The efforts aim to continue to enhance the SDR architectures to reduce WF portability cost over multiple SDR platforms.

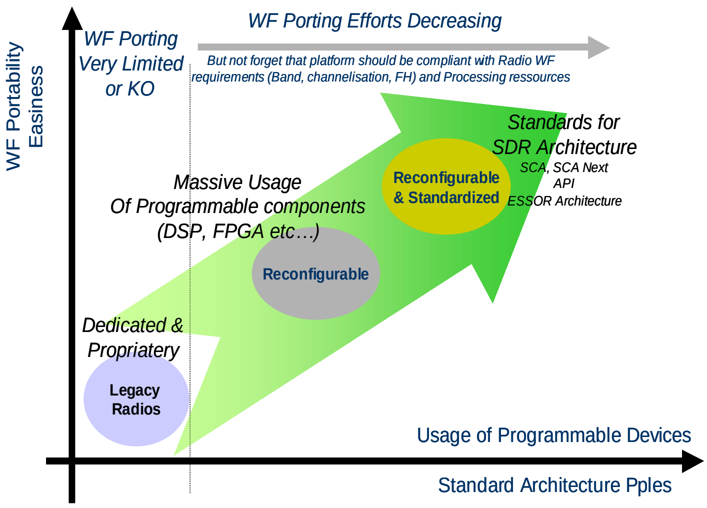

Figure 7 Standards for SCA Architecture

ESSOR Architecture[6]

ESSOR Architecture brings extensions and additions to the already published JTRS Radio Devices (RD) and Radio Services (RS) Application Programming Interfaces

[6] Refer to the ESSOR Architecture – Motivation and Overview presented at SDR'10 Wireless Innovation Forum Conference. http://groups.winnforum.org/p/do/sd/sid=2635

(API), including specification of a complete Transceiver API based from the WInnF Transceiver Facility.

One first essential technical addition of the ESSOR Architecture on top of JTRS achievements is the definition of coherent and complete Operating Environments for DSP and FPGA Processing Elements.

SCA Next [7]

According to JPEO JTRS, SCA Next is more scalable, lightweight, and flexible than SCA 2.2.2. It is compatible with radio sizes ranging from small, single channel radios to prime-power, multi-channel sets (Smaller Radios, Longer Battery Life, Faster Boot-up benefits for the warfighters). As a technology refresh, it incorporates advances in portability for Digital Signal Processor (DSP) and Field Programmable Gate Array (FPGA) processors and new design patterns for its Application Program Interfaces (APIs).[8]

Wireless Innovation Forum

The Forum has elaborated a Model for Coordination of International SCA Standards [9] organized around the Forum Coordinating Committee on International SCA Standards [10]. This model was developed for stakeholders (manufacturers, vendors, governments) of the international SCA-based ecosystem who seek increased harmonization among SCA-based international standards and is structured according to two mainstream axes:

- Coordination of International SCA Standards,
- Production of coordinated International SCA Standards, that include the Forum efforts in this area
  - SCA Next Working Group
  - Transceiver Facility Working Group
  - International Radio Security Services API Working Group
  - Smart Antenna Working Group

2.4 SDR Platform Capabilities

The SDR Platform consists of all the hardware that encompasses a radio in addition to the platform software. A given waveform application principally shall be able to execute on the radio platform.

To achieve this, three basic requirements have to be fulfilled:

- Compliance with an SDR architecture
- Compliance with a set of agreed APIs
- Hardware performance prerequisites

[7] http://sca.jpeojtrs.mil/scanext.asp
[8] JPEO JTRS Press Release 2nd December 2010
[9] Available at http://groups.winnforum.org/d/do/4673
[10] See Forum current projects on SDR standards at http://www.wirelessinnovation.org/page/Current_Projects

This latter requirement should not be forgotten: without such compliancy, an SDR radio platform compliant with SDR Architectures level and set of APIs, will not be able to run the required Waveform.

In contrast to generic COTS reference platforms, fieldable radio platforms are optimized (i.e. designed and built) for specific operational uses (e.g., man-pack radios are battery-driven and therefore designed for reduced power consumption). This implies that certain waveform applications or waveform implementations will not operate or operate with reduced performances on the constrained radio platforms.

Typical radio platform modules can have limitations in terms of Time domain, Frequency domain and Resources.

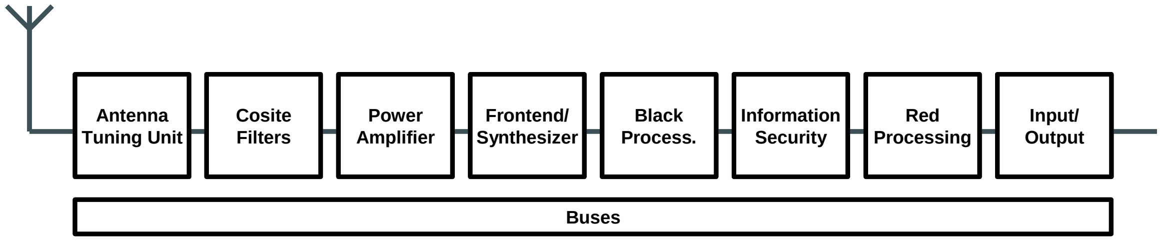

Figure 8 Principal Hardware Structure of a Radio

For example, the power amplifier may have limitations in ramping up/down times (time domain) and the frequency range (frequency domain). The internal buses are limited in latency and jitter (time domain) and in data throughput (resources).

The above examples outline clearly, that there are many different performance parameters which have to be determined for an SDR platform.

An engineering verification of a waveform application against the performance parameters of the SDR platform will provide an indication of the probability that the waveform application will be portable and execute properly on the radio platform.

3 SDR Technologies Improvement Areas

This White Paper, after providing some overview of Software Defined Radio (SDR) technologies for Tactical Communications Systems, highlights some key issues to be further addressed to increase the adoption of SDR technology by the market:

- Improving the WF portability: issues associated with Application Programming Interface (API) development,
- SDR Standards Compliance Certification
- Safety Certification
- Security aspects

3.1 SDR APIs Standards

The SCA defines architectural requirements on the Operating Environments (OE) of the tactical radio hardware (HW) and on the waveforms and other applications executing on the environment to facilitate the portability of the waveforms and applications between SCA-compliant platforms.

The SCA OE provides an abstraction layer via standardized program interfaces (i.e. API) between the radio platforms hardware and software based operating environment and the "portable" waveform software. The set of SCA APIs however did not include specific APIs for a number of different Devices (e.g. Serial, GPS, etc.) or Services (e.g. Networking, Retransmission, etc.).

As these APIs are required for the development of SDR products, the first JTRS production program was tasked with API development. In April of 2007 the JTRS JPEO released a subset set of these JTRS program APIs to the commercial and international community. The JTRS released APIs are accessible from the JTRS JPEO website address of: http://sca.jpeojtrs.mil/downloads.asp?ID=apis. Table 1 lists the released APIs.

Table 1 JTRS Released APIs

Table 1 JTRS Released APIs		
API		Description
1	AudioPortDevice	Audio Alert and Alarms, PTT and Stream (data) Interfaces
2	DeviceIO API	IO API for Devices
3	DeviceIOControl API	Request to Send interface
4	DeviceIOSignals API	Clear to Send interface
5	DeviceMessageControl API	Receive and Transmit and abort interfaces
6	DevicePacket API	Packet control interfaces
7	DevicePacketSignals API	Packet payload and signals interfaces
8	DeviceSimplePacket API	Packet dataflow payload interfaces
9	DeviceSimplePacketSignals API	Packet dataflow signal interfaces

Table 1 JTRS Released APIs

API		Description
10	EthernetDevice API	Ethernet API utilizes DevicePacket, DeviceIOControl, DeviceIOSignals and DevicePacketSignals APIs
11	FrequencyReferenceDevice API	Frequency Reference interfaces include 1PPS, and Time Figure of Merit
12	GPSDevice API	Global Positioning Service APIs
13	JTRS CORBA Types	Data types utilized in various APIs
14	MHAL API	Modem Hardware Abstraction Layer API
15	Packet API	Packet dataflow payload interfaces
16	SerialPortDevice API	Serial Device Packet and Control interfaces.
17	TimingService API	System and Terminal Time interfaces
18	VocoderService API	Vocoder (e.g. MELP, CVSD, etc.) interfaces.
19	MOCB API	MHAL On Chip Bus Application Program Interface
20	JTRS Platform Adapter	Platform Adapter interfaces

The JTRS public domain API release does not contain the complete set of APIs required to implement an SDR radio. Many of the APIs (e.g. Radio Security Services APIs) defined within the JTRS program are reserved for U.S. DoD usage only and are export restricted due to security concerns.

We also recognize that there are individual nation's policies which impose restrictions on the export of military radio technology. As a result of these restrictions, there are other projects (e.g. ESSOR or SVFuA) and organizations such as the WINNF that are working to define APIs that are not specified or otherwise commercially accessible.

As a consequence, a question arises: *How can this process be effective for SDR Customers and SDR manufacturers trying minimize their costs*[11]*?* We also have to consider the global defense environment, where other markets (e.g. Africa, Middle East, Asia, etc.) desire to utilize SDR technologies.

This emphasizes the necessity to have political agreements between nations to lower barriers preventing or limiting common International API standards. Political resolution will minimize the effort and cost of producing and delivering SDR technology and will promote and permit the exchange of different waveforms between nations. A particularly important aspect of the political agreement is the creation of a set of common security design requirements and API's which do not compromise national security requirements. The WINN Forum believes that a layered approach to these requirements and API's which include a common set extended by specific jurisdictional (e.g. NATO, EDA) and/or national requirements is one feasible approach to resolving this issue.

[11] Non-standardized or different approaches impact the portability of waveforms

3.2 SDR Standards Certification

Another important aspect affecting SDR development is the testing and certification of SDR products. Certification typically covers the procedures and the processes aimed at verifying the compliance of products against a set of standards such as the SCA. SDR certification verifies the compliance of radio platforms and software applications (i.e. Waveforms) to established SDR standards. The goals of SDR certification are to maximize application portability and interoperability between SDR platforms through standards compliance testing. With the spread of SDR concepts to different National tactical radio communities' issues regarding certification, certification bodies, and standards for certification has arisen.

SDR concepts for tactical radio systems introduce new aspects in the certification of SDR radios. The traditional certification goals of tactical radios are to guarantee the compliance of the over the air interface to relevant standards for interoperability or regulatory purposes. The certification of SDR equipment includes these tests but also needs to ensure that the development of the SDR product is performed in accordance with standards which to facilitate the development and portability of Waveforms and other tactical radio Applications as well as tests that the waveforms and applications conform to their requisite standards/specification The types of certification that are required include:

- Operating Environment (OE) certification which includes Operating Systems, Middleware and Core Frameworks
- Platform Devices and Services
- APIs
- Security Architecture and Design
- Waveform Information Assurance
- Waveform interoperability
- Platform Performance (e.g. emission conformance, etc.)

As a summary, the certification of SDR Platforms should provide and guarantee that the SDR Platform is capable of load, instantiate, tear-down, and unload waveforms developed to established SDR standards.

The certification of waveforms will provide the guarantee, that when the waveform is deployed on an SDR platform conforming to SDR standards that the waveform will be able to be, for example, loaded, instantiated, torn-down, and unloaded.

The above certification aspects are requested by Customers and Users to promote the development of value added applications, provide for reduced costs involving waveform portability and to reduce if not eliminate interoperability issues between military services and coalition partners. There are of course legal and regulatory issues involved with such certification.

The U.S. DoD has established the JTRS Test and Evaluation Laboratory (JTEL) organization to undertake formal SCA compliance testing for the JTRS Joint Program Executive Office

(JPEO) and DoD sponsored programs[12]. Processes, procedures and compliance testing tools have been developed by JTEL to validate that JTRS platforms and waveforms are compliant to JTRS SCA standards. In the U.S., separate waveform interoperability testing is performed by the Joint Interoperability Test Command (JTIC) for specific radio waveforms. It is not possible to have a non-JTRS radio certified to the SCA without a sponsor from within the US DoD and there is no other agency currently in existence anywhere which can certify an SDR to the SCA for either tactical or commercial radio applications.

The EDA (European Defence Agency) is analyzing SDR certification though a work group tasked with addressing the topic (managed by EU military representatives with support of European Industry) while in NATO there is not, at this time, any established group(s) for this purpose (but it is expected that this discussion will start in the near future).

We have to consider that for military use SDR systems typically will contain communication and transmission security measures among Nations. This requires that some activities need to be realized with National Agreements.

There is necessity to establish relationships between the different Certification Agencies that probably will be realized by different government agencies (one example is in the western alliance of NATO) to guarantee, for instance, that waveforms certified by NATO (or EU) certification agency should be considered certified for use on U.S. platforms and vice versa (this guarantees Cost Efficiency).

Wireless Innovation Forum activities in this important SDR Standards Certification topic are hosted in the "SCA Test & Certification" Working Group that is providing an industrial perspective of the SDR certification. A first report has been edited by the Forum, "Test and Certification Guide for SDRs based on SCA, Part 1: SCA"[13], and a new complemented edition is under elaboration.

3.3 Security

Security is an issue which spread across all topics related to SDR and may strongly influence the International Tactical Radio Market.

Security in SDR goes far beyond the topic of only the cryptography and addresses the following aspects:

- Confidentiality
- Integrity
- Authentication
- Availability

As the concept of SDR is providing possibilities to separate some of the security oriented tasks from others tasks, SDR could bring also opportunities to market radio products more easily on an international basis.

[12] These test facilities are not available to non- US DOD or commercial projects.
[13] http://groups.winnforum.org/d/do/1559

However this has to be considered carefully since modern waveforms make the security to spread over a significant part of the whole radio, and is not limited to “simple” Communication Security (COMSEC) features. For example, impact of pure waveform security aspects like Transmission Security (TRANSEC) should be examined.

Many customers now insist to implement national crypto by themselves, especially if the supplier is from a different country.

In this situation, exchangeable crypto devices / modules may be an interesting possibility for SDRs, because it decouples the radio from the crypto device/module.

Furthermore, Software Crypto would decouple the crypto devices / modules from the crypto algorithm, allowing it to realize different crypto algorithms in a common processing element, as into a Programmable INFOSEC module.

There are a number of issues regarding the suitability of a Programmable INFOSEC module for individual Nation’s use. To meet current policy and to allow internationally sourced SDR to be used to protect highly classified information and codeword (including Nation’s Eyes Only) it will likely be necessary to have a nationally-sourced cryptographic subsystem.

This would require detailed technical information about the SDR platform and, to minimize costs, a standardized security API to be available to allow implementation and security evaluation.

In order to exploit fully the encryption capabilities within military SDRs, National Security Agencies (NSAs) will have to successfully evaluate the SDR security architecture and INFOSEC sub-system. The nation’s NSA would also require the ability to sign INFOSEC module software loads. It is considered that the potential for the Nations to author and digitally sign national algorithms for use in SCA based military SDRs within the timescale of likely military SDR procurement is likely to be feasible.

However, there is concern that insufficient work may be in progress to be sure that this will be achieved in a common NATO/coalition manner necessary for effective waveform portability amongst different nations.

Therefore, to speed up this process it is necessary to define a common security strategy based on agreed interoperability and security scenarios, and defining which Security Architecture / Guidelines shall follow the development of SDR Base WF, SDR Platforms and Programmable INFOSEC module.

There are also barriers by the possibilities, which come into play with SDRs.

- It must be stated that if a business may represent a risk for the security interests of the potential customer the respective business attempts may not be successful.
- For nations it is often an issue if an SDR integrates code from other nations or integrates un-investigated COTS software.
- Recent discussions in the SDR community have shown that there are different positions in nations about this: some rigorously are rejecting foreign code in their SDR, others may accept in some areas forced by reality. Therefore, there is a need for a Mutual Trusting

Process in order to implement software from reliable and well known source. This is essential for many customers.

A key factor that can impact the SDR market is individual nation's policies for the export of military radio technology. For the few large nations, such as the US, which have a sufficiently large internal market with a large supply base this may be of little material concern. However, the majority of other nations (including the majority of European) nations have much smaller armed forces and, typically, a very small number of in country military radio manufacturers. Therefore both nations and industry have a need to access a larger market (nations to improve value-for-money during procurement and Industry to widen their customer base). The inclusion of INFOSEC and advanced features in military radios and particularly SDRs makes this more complex.

Challenges with international supply that can impact the SDR business include:

- Export restrictions – The majority of countries have strict export rules applicable to military equipments and information which require appropriate Government approval in relation to the suitability of the end user nation. Some nations will place tight control on the export of military SDR equipments, particularly those containing embedded INFOSEC through restrictive foreign military export sales (FMS) agreements. FMS supply arrangements established by some nations impose significant limitations on supplier industries and customer nations which may include:

    1. No commitment to particular supply timescales and long approval times from the supplying nation's Government.

    2. Restrictions on the use of the supplied equipment.

    3. Support arrangements requiring a return to country of origin with no guarantees on servicing times.

    4. Limited or no-access to detailed technical information without entering into restrictive Government approved Technical Assistance Agreements (TAAs).

- 'No foreign code' rule – Some nations have imposed this rule because of a belief that there is an inherent risk that SDR equipments or waveforms procured from foreign nations could include malicious code or security vulnerabilities which could lead to leaking of classified information or allow attack of the military communications network. The 'no foreign code' rule acts as a barrier to trade and therefore affects the SDR business model. However, in a world where COTS software is increasingly widely used in military systems, it is not clear that many nations can take such a position long term. It may be that as SDR technology matures the risks are better understood and such rules may be relaxed.
- Security Certification Data Requirements – Perceived new security risks with SDR technology are causing Nations procuring SDR equipments and waveforms to insist on wide ranging access to detailed technical information in order to allow them to be evaluated and certified for security. In particular, access to the full radio and waveform source code has been repeatedly mentioned in such discussions. This

places additional burdens (e.g. increased difficulty of obtaining export approval) and risks (e.g. protection of Intellectual Property (IP) on the supplying industry).
- Classification – In a number of cases there are differences between the classifications different nations would apply to particular elements of an SDR/waveform and this can add complexity to import/export.

SDRs have the potential to separate the supply of sensitive INFOSEC and waveforms from the supply of the radio system itself allowing more standard commercial arrangements to be used providing benefits to customer nations and more freedom of supply to industry. Whilst this approach is certainly not mature there are signs that it may be a solution with some vendors offering export models of their radios or variants where the INFOSEC can be specified by separate agreements. However, a precursor to making this approach work is the international standardization of Security APIs and some agreement on the security accreditation approach.

Wireless Innovation Forum activities: As the Wireless Innovation Forum considers these aspects as important, some dedicated working groups have been established (see Forum current projects at http://www.wirelessinnovation.org/page/Current_Projects) : Security Work Group and the International Security Services API Task Group (ISS-API).

- The Security Work Group has edited the “Securing Software Reconfigurable Communications Devices”[14] document that is intended to provide guidance, key considerations and recommendations for SDR developers and manufacturers regarding the design and manufacturing processes essential to producing appropriate security solutions for software reconfigurable radio platforms.

- The International Security Services API Task Group is finalizing development of an "International Security Services API". This specification is being developed for nations, international organizations and companies who need software interoperability and portability between international and independently developed software radios. The international radio security services API will specify how to interface and operate with a common set of radio security services improving interoperability and portability of software through the use of a common open software architecture.

3.4 Safety certification

It’s easy to figure out that the future expectation for SDR technology in the avionic market, for both military and civil aircrafts (fixed or rotary wing), are about the use of this technology for any application which implies RF signal transmissions and receptions.

Because for the time being we can keep RADAR applications out of the scope of this document, we should focus on those applications which imply a “collaborative” exchange of information through the RF. By this classification we include radio communications, radio navigation and identification.

[14] http://groups.winnforum.org/d/do/3014

Today's examples of these applications are:

- Communications: any kind of military communications and data link which can be done in HF, UHF, SHF etc., but also civil communications and data links (e.g. those with the local Civil Aviation Authority for Air Traffic Control, with the Airlines, etc.)
- Navigation and landing: VOR[15], DME[16], GBAS[17], SBAS[18], ILS[19], MLS[20], etc.
- Identification: military IFF modes, civil ones, TCAS[21], etc.

All of the above are more than natural candidates to be SW waveforms which should run in avionic SDR platforms. It could be criticized that many of those applications could be out of the scope of this Special Interest Group, but military aircrafts and helicopters are indeed included in Tactical networks because always they have had (and, if necessary, with the NCW concept, they even more are) to interoperate with naval and ground assets through radio communications. Military aircrafts need more and more to share civil controlled airspaces with commercial aircrafts and this is due at least to two important factors:

1. military segregated airspaces are being more and more reduced in favor of an increasing demand in commercial air traffic which is foreseen to double in 10-15 years;
2. modern tactical scenarios more and more imply force projections (which means long flight transports), and air assets are often re-dislocated in other countries from which they have to fly over neutral countries in order to reach the theatre of operations.

For the above needs, military aircrafts have to be compliant to the same rules for safety flights as well as the commercial aircrafts. In other terms their communications equipments (at least those by which they communicate with the local CAA[22]), radio navigation and identification equipments have to be certified for safety of flight by that CAA (or have an internationally recognized certification), or they won't be allowed to fly over that countries. This is already valid today and will more and more be valid tomorrow with the foreseen 4-dimensional Air Traffic Management (see NextGen and SESAR Programs respectively in US and Europe) for Commercial aviation.

A military aircraft will have to comply with safety certification rules for its ATC VHF waveform because its flight will have to be coordinated with local air traffic by the local CAA, for its VOR and DME waveforms because its navigation systems shall be affordable like the civil ones when under the CAA control, for its ILS waveforms because if an emergency landing will be needed the system shall comply with (and shall be certified to) the same safety requirements as the commercial aircrafts do, etc.

Therefore once Software Defined Radio channels will be available onboard a military aircraft a natural expectation will be to de-install all conventional radios, radio-navigation and identification equipments in order to manage them through SW waveforms on SDR platforms,

[15] VHF Omni-directional Radio-range
[16] Distance Measuring Equipment
[17] Ground Based Augmentation System
[18] Satellite Based Augmentation System
[19] Instrumental Landing System
[20] Microwave Landing System
[21] Traffic Collision Avoidance System
[22] Civil Aviation Authority

and so to extend the same advantages for logistic, life cycle cost, etc., also for those applications.

Actually if the possibilities offered by the SDR technology in terms of money savings are considerable in a ground platform, they can even be much greater onboard of an airborne one, because:

- Different phases in a mission of an aircraft exclusively need different waveforms (e.g. landing waveforms are only needed during landing, when cruise navigation waveforms are not, etc.);
- all the avionics architecture design principles (for the new aircrafts) are going through a total revision, that means that federated architectures are going to disappear in favor of distributed ones with a standard hardware to run upon; therefore because the aim is to have total re-configurability of any function of the avionic system there won't be room for islands of federated architecture;
- some platforms (like fighters, light helicopters, UAVs) have stringent requirements in terms of space available, electrical power, heat dissipation, so using standard platforms on which being able to reconfigure SW applications according to the needs could be very important for the platform roles, performance and capabilities to be upgraded during its life.

For the above reasons it's a natural market expectation to manage both military and civil waveforms by SDR platforms onboard of aircrafts. On the other hand, it has been also described that the performances of these new couples (civil waveforms + SDR platforms) shall be the same in terms of safety for flight.

4 Conclusions

This document has shown the importance of having strong standards that:

- Shows the market stakeholders the benefits and return on investments that the SDR technology can provide.
- Provides maturity to the technology
- Supports the implementation of SDR equipment.

In order to achieve those objectives it's necessary to have the commitment of the current SDR developers into a common and complete SDR standard, which means:

- Operating environment: The operating environment will include the Core Framework, the POSIX profile and the connectivity middleware.
- API's: It's suggested to increase the capabilities of the existing API's. The document has presented the current set of APIs released by the JTRS, but also the lack of information in some SDR areas. This situation can significantly increase the porting efforts and the cost.
- DSP and FPGA environment: The current SCA (OS, POSIX, Middleware) specification does not fully cover all radio processing elements (e.g. FPGA, DSP, etc). Assessment of FPGA and DSP functionality is based on "experience" rather than some form of guidance, formal criteria, or standard.

The ongoing initiatives, ESSOR Architecture and SCA Next, aim to extend and improve the SCA reference architecture to enhance Waveform portability in SDR technology.

The Wireless Innovation Forum, through its Steering Committee on International SCA Standards (see Press Release 29th July 2010 announcing its set up [23]) and its SCA technical committee, developing and contributing to these improvements, is a key actor. Especially, in a Press Release, 18th Feb 2010[24], the Forum announced its support for a "three category" approach in the evolution of the Software Communications Architecture (SCA) and related standards.

The Forum's recommendation is modeled on a proposal made by the European Defense Agency's (EDA) during SDR'09, the Forum's annual technical conference and product exposition held Dec 1-4, 2009. The recommendation allows for future developments of the SCA base specification, application programming interfaces (APIs) and other necessary extensions to occur in a coordinated manner across the international community Wireless Innovation Forum Makes Recommendation on the Evolution of the SCA.

Regarding the SDR certification aspects, nowadays the only certification initiative is lead by US, enabling the JTEL laboratory to certify the SCA platform and the SCA waveform

[23] Wireless Innovation Forum Press Release – 29th July 2010
http://www.businesswire.com/news/home/20100729006161/en/Wireless-Innovation-Forum-Announces-Steering-Group-Coordinating

[24] Wireless Innovation Forum Press Release – 18th February 2010
http://www.businesswire.com/portal/site/home/permalink/?ndmViewId=news_view&newsId=20100218006690&newsLang=en

compliance. However, it's necessary to globalize the efforts on SDR certification and get other countries involved in these efforts.

Following this statement, there are two more initiatives launched recently:

- EDA – ESSaC (European SDR Standardization and Certification) Study. The study on SDR certification and standardization within Europe has conducted by the EDA in2010 with the objective of settling the basis of the European SDR certification infrastructure.
- WINN Forum. The Wireless Innovation Forum launched the Certification and Testing Working Group, in order to provide an industrial perspective of the SDR certification. The main output of this group is the "Test and Certification Guide for SDRs based on SCA, Part 1: SCA".