PUBLIC SAFETY
PSWN PROGRAM
WIRELESS NETWORK

Saving Lives and Property Through Improved Interoperability

Software Enabled Wireless Interoperability Assessment Report— Software Defined Radio Subscriber Equipment

FINAL

March 2002

Table of Contents

EXECUTIVE SUMMARY

The public safety community continues to face daily interoperability challenges. Many public safety radio systems operate on different frequency bands and with incompatible technologies. To address these and other interoperability challenges, the Public Safety Wireless Network (PSWN) Program created programs such as the Public Safety WINS: Wireless Interoperability National Strategy to identify technical solutions for improving interoperability (e.g., WINS identifies multiband, multimode radios as one such solution). Software defined radio (SDR) technology has been widely recognized as a promising technology to implement multiband, multimode radios.

This report assesses the overall state of SDR technology as it applies to the public safety land mobile radio (LMR) environment. It focuses on SDR subscriber equipment and identifies the marketplace, regulatory issues, the technology, and impacts of SDR technology on the public safety community.

The Marketplace

Most LMR equipment vendors have not conducted extensive research and development of SDR technology specifically for public safety applications using subscriber equipment. However, preliminary findings show that the military community has invested the most time and effort in SDR development; in comparison, the commercial community has done a relatively small amount of SDR technology development. The military community has been a strong supporter of SDR technology since the early 1990s, and the commercial industry has recently begun to realize the benefits that SDR technology offers. Although SDR technology has been considered, the public safety community has not yet engaged in development activities to explore SDR technology. To date, traditional LMR vendors have not invested resources in developing SDR products for the LMR environment. SDR technological advances are promising; however, more information is needed to provide better insight into the LMR vendors' development time-lines and cost estimates.

Impacts on the Public Safety Community

Because SDR technology is still in its infancy, it is unlikely that SDR subscriber devices will be available for public safety in the near future. However, the public safety community should leverage the research and development of products the military and commercial communities are currently undertaking. As the SDR technology matures, the public safety community could gain the following key benefits—

- Interoperability across dissimilar radio networks, frequency bands, and technologies
- Simplified user interfaces allow users to operate a single SDR device on systems with disparate technologies – beneficial to the public safety community especially during emergency situations
- Streamlined security across multiple radio network technologies

- Access to enhanced data applications (e.g., remote access to crime databases) due to the ability of a single SDR device to operate with multiple wireless data protocols (e.g., Cellular Digital Packet Data [CDPD] and Radio-Data Link Access Protocol [RD-LAP]).

SDR technology, as it applies to the public safety community, is not without risks. Risks to the public safety community associated with SDR technology implementation include—

- Potential interference that could impact the integrity of existing radio systems
- Difficulty establishing open standards with existing proprietary systems
- Vulnerability due to unauthorized access to the software-based device.

The Regulatory Landscape

Recently, commercial interest in SDR technology has prompted the attention of regulatory agencies. The National Telecommunications and Information Administration (NTIA) and the Federal Communications Commission (FCC) have closely monitored the latest advances in SDR technology. These regulatory agencies are specifically concerned about potential interference issues introduced by SDR subscriber equipment because it is speculated that existing radio systems will experience interference from SDR devices. SDR technology introduces several challenges for spectrum management, prompting the need to establish guidelines to ensure that SDR devices adhere to regulatory requirements.

The SDR technology guidelines established by the FCC include a streamlined equipment authorization process. However, because of the immaturity of SDR technology, the FCC requires extensive hardware and software testing. This testing is intended to protect current radio systems, ensuring that interference is prevented. Each software application under which SDR devices will operate must be tested for regulatory compliance. The strict guidelines for SDR technology established by the FCC could extend the development timeline for SDR devices.

Software Defined Technology

Originally, the military community developed SDR technology to support global communications. More recently, the commercial community has shown interest in developing SDR technology. It is likely that the military and commercial developments for SDR technology will be incorporated into LMR products.

SDR devices have the capability to dynamically change transmitter and receiver characteristics without changing hardware. Unlike traditional radio devices, SDR subscriber equipment relies on digital signal processing (DSP) chips for modulation and filtering. An SDR device is envisioned to operate with the existing and evolving LMR system by automatically switching operational modes.

***

SDR technology has the potential to considerably reduce the interoperability gaps that currently exist within the public safety community radio networks. This technology holds the promise of offering advanced features and capabilities not available in current LMR systems. However, SDR technology is still at an early stage of development. There are still many proprietary design, spectrum management, and communication security issues that must be fully addressed.

1. INTRODUCTION

This report provides an assessment of the SDR technology as it applies to the public safety community. Although the military community has realized many benefits from recent advances in SDR technology, the land mobile radio (LMR) equipment vendors have yet to use SDR technology. This report presents an overview of the SDR marketplace, the potential risks and benefits of implementing SDR technology on LMR subscriber terminal equipment for use by the public safety community, and analysis on recent rulings and guidelines published by the Federal Communication Commission (FCC) that will influence the continuing development of SDR technology.

1.1 Background

LMR networks provide wireless communications for local, state, and federal public safety communities. The existing LMR networks are based on a wide range of technologies. Typically, most LMR networks operate across disparate frequency bands and multiple technologies, introducing interoperability challenges. The advancements of intelligent network (IN) technology have allowed for the possibility to distribute computing to all network elements (rather than processing from a centralized location). The application of IN-based technology will likely result in a fundamental shift of network topology from existing disparate LMR architectures to more flexible interoperable architectures. The distribution of processing in the IN environment will occur across all network elements, including subscriber equipment. This intelligent subscriber equipment will be made possible by SDR technology.

1.2 Organization of Report

This report consists of six main sections, including this introductory section. Section 2 presents an overview of the SDR marketplace, including projected timelines for the development of devices. Section 3, SDR Technology in the Public Safety Community, summarizes the advantages and risks associated with SDR technology as it is applied to LMR subscriber equipment in the public safety community. Section 4, Regulatory Landscape, summarizes the FCC's recent rulings and guidelines regarding SDR technology. Section 5, SDR Technical Discussion, describes the basics of SDR technology and the development path for SDR devices. Section 6, Conclusions, presents key findings.

2. SDR MARKETPLACE

The PSWN Program assessed the current SDR subscriber equipment marketplace for this report. The key findings of the marketplace assessment indicate that SDR technology research and development efforts are segmented across three major communities: military, commercial wireless, and public safety. Preliminary findings indicate that the military community has committed the greatest effort and time researching and developing SDR products (more than 10 years).

SDR technology innovations have stimulated interest throughout the commercial industry. However, the commercial sector is only now beginning to realize the benefits of their SDR technology research efforts. It is anticipated that commercial offerings of SDR subscriber devices will be developed specifically for the consumer marketplace. The requirements of SDR devices for the commercial wireless sector are based on enhanced applications with the primary intention of generating revenue for wireless service providers.

2.1 Current SDR Marketplace

Figure 1 shows the marketplace migration path for SDR subscriber equipment technology. In the military community, development of SDR products began in the early 1990s and is now entering an implementation-ready state. It is anticipated that the commercial and public safety communities will continue to develop and eventually implement SDR devices; the SDR Forum[1] ***optimistically speculates*** that SDR devices will be ready for deployment by 2005.

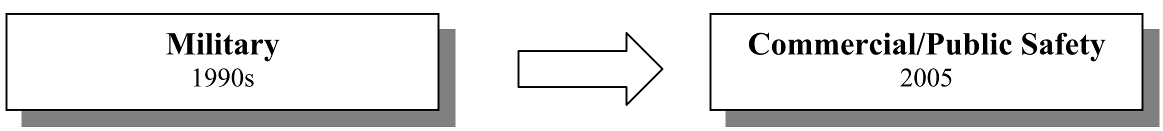


Figure 1
Projected SDR Timeline

There are benefits associated with the relatively long timeline for the development of SDR technology specific to the public safety community. One such benefit is that the public safety community can leverage and apply lessons learned from the research and development efforts already invested by the military and commercial wireless communities. In particular, the SDR technology developed and used by the military will benefit the public safety community because the communities share similar operational and mission requirements. Appendix C contains a sample set of requirements that the public safety community could have for SDR devices. These sample requirements are typical for any advanced radio system exclusively designed for administrative and tactical use by the public safety community.

---

1 *The following discussion on the SDR Forum is adapted from the SDR Forum web page - http://www.sdrforum.org/executive_summary.html*

The SDR Forum is dedicated to supporting the development, deployment, and use of open architectures for advanced wireless systems. To that end, the Forum helps to:

- Accelerate the proliferation of enabling software definable technologies necessary for the introduction of advanced devices and services for the wireless Internet

- Develop uniform requirements and standards for SDR technologies to extend capabilities of current and evolving wireless networks.

The Forum continues to attract members from industry, academia and government, with global representation from Asia, Europe, and the Americas. This includes many new members that have SDR products to offer the market. A listing of current members of the SDR Forum is included in Appendix B.

The SDR Forum has multiple working committees to aid in the advancement of the development of SDR technology. SDR Forum's working committees are:

- **Regulatory Committee** – Chartered to promote the development of a global regulatory framework supporting software download and reconfiguration mechanisms and technologies for SDR-enabled equipment and services. The Regulatory Committee's milestones include the submission of comments to FCC Notice of Inquiry Response and Notice of Proposed Rulemaking on behalf of the Forum. Next Steps of the Regulatory committee include the continual support of international regulatory issues.

- **Markets Committee** – Chartered to raise industry awareness through public relations activities, including published articles, press releases and representation at industry trade shows; to increase and maintain Forum membership; and to collect and analyze market data on all industry segments. The Markets Committee milestones include reaching the 100-member mark; developing collateral material for member use in outreach activities. Next Steps of the Markets Committee include continual member outreach and Forum promotion and sponsoring a market research update.

- **Technical Committee** – Chartered to promote the advancement of software-defined radios by using focused working groups to develop open architecture specifications of hardware and software structures. Within the Technical Committee, there are specific working groups that deal with different aspects of SDR technology. The working groups of the Technical Committee are: the Download/Handheld working group, the Base Station/Smart Antennas working group, and the Mobile working group.

- The Download/Handheld working group was chartered to promote the use of software defined radio technology in handheld terminals, providing dynamic reconfiguration under severe constraints on size, weight, and power. The Download/Handheld working group's milestones include the completion of use-cases for handhelds and formation of liaison with the Third Generation Partnership Project – Mobile Execution Environment (3GPP-MExE) and the Wireless Access Protocol (WAP) Forum. The next steps of the Download/Handheld working group include submitting a proposal for MExE2000 release at the joint SDR/MExE meeting August 29-30, 2000

- Base Station/Smart Antennas working group was chartered to promote the use of software defined radio and reconfigurable adaptive processing technology in wireless base stations worldwide for terrestrial, satellite, mobile, and fixed services. The Base Station/Smart Antennas working group's milestones include developing a new work plan and merging all the past efforts of the Smart Antenna working group into one offering. The next steps of the Base Station/Smart Antennas working group include updating and revising a technical report of base stations and smart antennas based on results of use cases completed by the Mobile working group

- Mobile working group was chartered to promote the use of software defined radio technology in commercial and military applications where station mobility, dynamic networking, and functional flexibility are required; identify and maintain the collection of recommended wireless, network and application interface standards to meet these objectives; and develop and promulgate new standards as necessary. The Mobile working group's milestones include the drafting of SDR architecture performing in military systems. The next steps of the Mobile working group is to continue working with the Base Station working group to identify common areas of architecture reuse, implement one common software radio application for architecture tests, and to continue to revise and test SDR architectures.

The traditional LMR equipment vendors (e.g., Motorola, Thales [formerly Racal], EF Johnson) have not formally announced forecasting timelines for the development of SDR products. Although no formal timelines have been set, these traditional LMR equipment vendors, among many other entities, are considering SDR technologies and are involved in the SDR development arena. The Request for Information (RFI) process[3] could be utilized to provide detailed information regarding vendor offerings of SDR technology. The information gained through the RFI process could include subscriber equipment development time-lines and projected cost estimates. Table 1 identifies the subscriber equipment vendors and their current involvement in SDR technology research and development.

[2] *The Request for Information Process is a common industry practice to gain knowledge on specific subject. In the RFI process, information and other comments are solicited from the public regarding the particular topic.*

Table 1
Manufacturer Subscriber Equipment

Subscriber Equipment Vendor	Land Mobile Radio Equipment		Software Defined Radio Activity		
	Multimode Subscriber Terminal	Multiband Subscriber Terminal	SDR Forum Member	Military Subscriber Terminal	Commercial Subscriber Terminal
Datron	Yes	Yes	No	No	No
EF Johnson	Yes	Yes	No	No	No
General Dynamics*	Yes	Yes	Yes	Yes	No
Harris	Yes	Yes	Yes	Yes	No
Lucent Technologies	No	No	Yes	No	Yes
M/A-COM**	Yes	Yes	No	No	No
Motorola	Yes	Yes	Yes	Yes	Yes
Nokia	No	No	Yes	No	Yes
Kenwood	No	Yes	No	No	No
THALES formerly RACAL	Yes	Yes	Yes	Yes	No
Raytheon	Yes	Yes	Yes	Yes	No

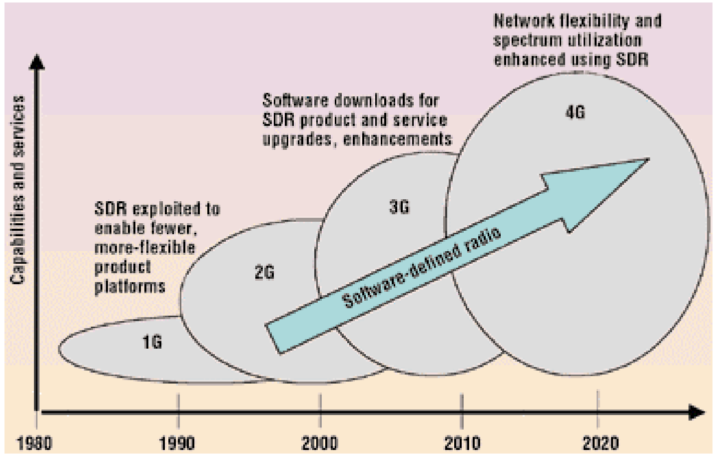
* General Dynamics purchased Motorola's Government Systems division that is developing SDR products for the military

** M/A-COM includes both OpenSky and EDACS

The data in Table 1 shows that the dominant LMR equipment providers are also active participants in the SDR interest groups. This indicates that a possible intersection exists between the future LMR subscriber equipment and SDR technology. A complete list of SDR forum members is included in Appendix B.

2.2 The Future of SDR Research

Currently, there is very little published data supporting the timelines for the development of SDR technology to be applied in LMR subscriber equipment. Most data available is specific to commercial offerings of SDR technologies. This data is still valuable to the public safety community because these commercial SDR offerings will affect all the communities considering SDR technologies as part of their wireless communications strategy. Although public safety SDR offerings will not become a reality until well after commercial SDR offerings are established, the public safety community could still benefit. The public safety community can leverage future commercial SDR offerings as they become available – at least until public-safety-specific SDR equipment is developed and implemented. Figure 2 presents a view of the projected timeline of the potential capabilities and services that may be possible with SDR technology. Table 2 provides a sample of potential services and applications, as they apply to each user community, which may become possible with the implementation SDR technology.



source: Software Defined Radio Forum

Figure 2
SDR Capabilities and Services Timeline

Table 2
Potential Services and Applications

Military	Commercial	Public Safety
• Secure, encrypted communications • Mission flexibility • Options to select communications channel by availability • Real-time flexibility • Portable command post • Integrated radio, router, and computer • International connectivity to prevailing networks	• International connectivity • Location awareness • Multimedia applications • Virtual private networks—Closed user groups • Media distribution • Combined delivery of e-mail, voice mail, messages, and faxes • Browser capability	• Nationwide portable station for response crisis management • Improved emergency communications by the use of one device that can operate on multiple systems • Closed user groups • Database access • International connectivity (especially for Federal use and search and rescue operations)

3. PUBLIC SAFETY ENVIRONMENT

This section addresses the key areas in which SDR technology will affect the public safety environment. It focuses on describing the following areas, highlighting benefits and risks:

- Interoperability
- Spectrum management
- User interface
- Communications security
- Data services.

3.1 Interoperability

Public safety interoperability, simply defined, is the ability of public safety personnel to communicate with staff from other agencies, on demand and in real time. Today, public safety agencies confront a multitude of situations in which interoperable communications is critical, including emergency responses to natural and manmade disasters, civil disturbances, and terrorism (both foreign and domestic).

To address interoperability issues, the PSWN Program developed the Public Safety Wireless Interoperability National Strategy (WINS). Public Safety WINS is the PSWN Program's road map for improving interoperability among public safety wireless networks around the Nation. Public Safety WINS has identified multiband, multimode radios as a possible technical solution for improving interoperability. SDR has been widely recognized as a promising technology to achieve multiband, multimode radios.

The key benefit of SDR technology to public safety is interoperability across disparate radio networks, frequency bands, and technologies. Although the potential benefits to interoperability are paramount, SDR technology could also impact other areas such as spectrum management, standards, security, and data applications. The impacts that SDR technology will have on these additional areas are discussed in this section.

3.2 Spectrum Management

Great strides have been made in the development of SDR technology, and only now are the spectrum management issues beginning to be addressed. While current and near-term SDR implementations permit easy changes to the radio's fundamental characteristics (e.g., transmit power, encryption schemes, modulation type) through software changes, the development of an adaptable SDR device that surveys the spectrum and automatically determines what frequency and other types of radio characteristics it should use to communicate is a long-term goal for the future. This type of automatically adaptable SDR device will pose the greatest challenge to spectrum managers and regulatory agencies.

Public safety radio channels are isolated and located noncontiguously in various areas of the frequency spectrum. Table 3 shows the public safety spectrum allocations, which are fragmented into eight radio bands.

Table 3
Public Safety Frequency Bands

Bands	Frequency Range (MHz)	Channel Distribution (%)*
Low-band VHF	25–50	16
Low-band VHF	72–76[4]	1
VHF	150–174	33
VHF	220–222[5]	1
UHF	406.1–420	18
UHF	450–512	21
700 MHz	764–776 and 794–806	0
800 MHz	806–824 and 851–869	10

* The recent allocated channels in the 700 MHz band are not factored in the calculation.

It is apparent from Table 3 that the public safety frequency allocations are widely distributed and sectioned into different frequency bands. These frequency bands are generally narrow and are isolated from one another—creating radio environments that cannot easily share radio communications and that are congested. Unfortunately, these public safety frequency bands will continue to exist because moving all public safety agencies to a contiguous band would be difficult.

Moving forward, as SDR technology continues to advance, so will the processes for conducting spectrum management. In today's LMR system, spectrum managers have to allocate specific frequencies for each voice channel that will be used in a specific system. A significant challenge is to reduce or eliminate any interference with other radio systems. The same challenge will hold true for SDR devices. The main difference, and the greatest consideration for conducting spectrum management with SDR devices is the ability for one SDR device to operate on multiple frequency bands. SDR could introduce harmful interference, which is unacceptable to the public safety community. Mixing SDR devices and traditional radios in a same frequency band could create spectrum issues if not properly managed. To prevent interference from affecting existing users, extensive field-testing of SDR technology is required, which will likely lengthen the time to market.

3.3 Standards

Public safety radio systems suffer from incompatibility problems because of the proprietary nature of some vendor equipment. Project 25 was established to standardize LMR interfaces and network devices, and compliance improves interoperability among newer digital systems. Older systems were not built to comply with Project 25 standards and thus often are not interoperable with each other or with new systems. Although there are many advantages of standards-based radio systems, not many public safety radio systems are Project 25 compliant. Many of these existing public safety radio systems are older and most agencies operating these

---

[4] *Bands 72-76 are authorized for use of firecall box operations on a shared basis with industrial business*

[5] *According to FCC dockets 47CFR 90 parts 717, 719, and 721 address the 220-222 MHz frequency bands.*
717 – allocates three 10 block channels (51-60, 81-90, and 141-150) for non-government mobile fixed use
719 – allocates 181-185 for emergency medical use (public safety/mutual aid channels)
721 – allocates the remaining channels for non-nationwide radio systems in the 220-222 MHz frequency bands

systems are not in a position to buy new systems. This adds to generalized system incompatibility, which continues to be a common challenge across all levels of government.

Because SDR devices can potentially operate with incompatible technologies, they can relieve the immediate need to install new, common standard, systems to ensure compatibility. However, the SDR Forum envisions that a standards process will be established for SDR technology, providing a unique opportunity for the public safety community to identify their SDR requirements to be included in future offerings of SDR devices. An open SDR standard could eventually create more competition in the LMR marketplace and possibly drive down LMR equipment prices.

3.4 User Interface

The user interface is a critical element for public safety users because they depend on easily accessible radio communications during emergency situations to help save lives and protect property. Public safety users demand radio user interfaces that are simple to use, easy to navigate, and easy to learn. Unfortunately, because of incompatible systems, public safety users often carry multiple radios during emergency and police cars commonly have multiple radios installed in them as a makeshift interoperability solution. It is not uncommon for each different radio to have a unique user interface.

SDR devices can have simple user interfaces because multiple radios are consolidated into a single device. However, if it is not designed properly, the user interface could become a major obstacle to effective communications. Because SDR is software upgradeable, it provides an opportunity to incorporate new technologies that could help simplify user interfaces. The most notable example is voice-activation technology that allows users to control radios hands free.

3.5 Communications Security

Increasingly, state and local law enforcement agencies recognize the need to have secure communications because clear communications can be easily compromised. Most federal law enforcement agencies already have encryption capabilities and are in the process of transitioning to Project 25-compliant encryption schemes.

Encryption in LMR systems adheres to the applicable U.S. Government standards published by the National Institute of Standards and Technology (NIST), for unclassified information and Information Security (INFOSEC) mandates by the National Security Agency (NSA) for classified information. Encryption for classified information is considered Secure and is referred to as Type I and Type II cryptographic encryption. Encrypted communications for unclassified transmission and reception of LMR communications is known as Type III and Type IV encryption. Encryption to meet these respective standards can be achieved via digital transmissions, which consists of a family of proprietary and standards-based algorithms that use the Data Encryption Standard (DES) as the "engine" of the encryption module. Most all encryption subsystems operate with 'keyed" inputs, which are digital bit streams known as key variables. For voice traffic encryption, a single key variable is assigned to transmitting and receiving units to operate in the encrypted, or "coded" mode.

Key management is the process by which keys are generated, stored, protected, transferred, loaded, used, and destroyed. Key management doctrine in an organization addresses the organization's policy for managing encryption keys. All encryption keys, whether Type I or less must be protected against unauthorized access, and procedures must be in place to safeguard all cryptographic elements. Keys can be loaded manually or over the air. Manual key loading occurs when key variables are physically loaded into the radio via a loading device (typically using a microprocessor that is physically connected to the radio). Radios can also be brought to a maintenance facility for re-key. Over-the-air-Rekeying (OTAR) allows rekeying of radios over an air interface. OTAR is a Key Management program that is implemented from a centralized key management controller over an LMR channel.

SDR subscriber equipment presents advantages for secure communications in LMR networks. However, the NSA and NIST carefully scrutinize any development leading to software implementation of different algorithms. The processes and physical and electronic security of encryption and decryption and OTAR are carefully controlled and implemented to prevent unauthorized access and spoofing. Sending algorithms over the air, or even entrusting them to manual devices is a security risk that requires more robust levels of physical security and anti-spoofing protection.

3.6 Data Services

Public safety agencies increasingly rely on data communications in their daily operations. Some notable wireless data applications are National Crime Information Center (NCIC) queries, transmission of fingerprints and mug shots, terminal-to-terminal messaging, local crime information data queries, telemedicine data, and report writing. To date, these data applications are commonly implemented on data networks separate from the voice communications network. Anticipating that data services will play a significant role in future public safety communications, the Project 25 steering committee has begun developing high-speed data standard Project 25/34 for public safety applications.

SDR devices could eliminate the need for separate data networks. It is envisioned that SDR devices would provide integrated voice and data (IV&D) capabilities that send voice and data information over the same channel to radios in the field. IV&D uses the idle airtime between voice transmissions to send data information on the same radio frequency (RF) channel, thereby eliminating the need for additional channels for data.

In the long run, SDR technology would expand data applications to include, for example, location tracking, multimedia delivery, and telemedicine. SDR technology provides the flexibility to implement these new services through software upgrades. These upgrades will be much faster and simpler than making those same upgrades with hardware modifications.

4. REGULATORY LANDSCAPE

The NTIA and the FCC have closely monitored the latest advances in SDR technology. These regulatory agencies are specifically concerned about potential interference issues introduced by SDR subscriber equipment because it is speculated that existing radio systems will experience interference from SDR devices. Specifically, concern focuses on the ability that software-enabled technology provides to allow subscriber terminal equipment to dynamically reconfigure its transceivers characteristics without user intervention. SDR technology introduces several challenges for spectrum management, prompting the need to establish guidelines to ensure that SDR devices adhere to regulatory requirements.

The FCC has implemented the standard rule-making process to establish the regulatory and operational guidelines for SDR technology. The regulations and operational guidelines for SDR technology began with the FCC issuing a Notice of Inquiry soliciting comments from the public in March 2000. After incorporating these comments, the FCC issued a Notice of Proposed Rulemaking for additional comments in December 2000. The FCC established the first phase of rules for SDR technology in its First Report and Order—September 12, 2001. It is anticipated that the FCC will establish additional rules for SDR technology as the technology evolves. Notably, the rules established on September 12, 2001, did not fully address the public safety community's main concerns associated with software-enabled technology—

- Potential unintended harmful interference and unauthorized frequency access
- Security and vulnerability issues introduced with dynamic transceiver configuration.

The ruling did create a new equipment classification (Class III) specifically to categorize SDR devices. The ruling also included guidelines that promote a streamlined equipment authorization process. This policy change gives equipment manufacturers the ability to modify the frequency, power, and modulation of SDR devices without filing a new equipment authorization application for each change. Table 4 contains the major points of the First Report and Order of September 12, 2001, which will be incorporated into law if the general public does not submit petitions for appeal.

Table 4
Overview of FCC First Report and Order (September 12, 2001)

Proposed Rule Changes	Description
Definition of Software Defined Radio	• Proposes to define an SDR as a radio that includes a transmitter in which the operating parameters of the transmitter, including the frequency range, modulation type, or maximum radiated or conducted output power can be altered by making a change in software without making any hardware changes
Class III Permissive Change	• Class III changes require submission of test data proving that the equipment complies with the applicable requirements for the service(s) for which the equipment will operate.
Equipment Authorization Requirements	• Class III permissive changes are authorized through a streamlined filing procedure that does not require the filing of a complete application form with each change.
Electronic Labeling	• This option allows SDRs to be equipped with an electronic label that displays the FCC identification number

The SDR technology guidelines established by the FCC include a streamlined equipment authorization process. However, due to the immaturity of SDR technology, the FCC requires extensive hardware and software testing. This testing is intended to protect current radio systems, ensuring that interference is prevented. Each software application under which SDR devices will operate must be tested for regulatory compliance. The strict guidelines for SDR technology established by the FCC could extend the development timeline for SDR devices. Since the ruling of September 12, 2001, does not address all the issues of SDR technology, such as spectrum management and security, it is anticipated that the FCC will establish additional rules for SDR technology as the technology evolves.

5. SOFTWARE DEFINED RADIO TECHNOLOGY

This section provides a brief overview on software defined radio technology and introduces SDR subscriber equipment.

5.1 Definition of SDR

An SDR device (e.g., portables and mobiles) allows users to change transmitter and receiver characteristics such as modulation type, wideband and narrowband operations, radiated power, and air interfaces by making software changes without any hardware alternation. Traditional LMR devices are based on specialized hardware such as transistors and integrated circuits. In more modern LMR radios, digital signal processor (DSP) chips are used for analog-to-digital and digital-to-analog conversion of the radio transmissions. A DSP chip is a real-time digital signal processor that can alter its functionality by executing different software algorithms.

Recent advances in DSP chip design and fabrication will allow for more advanced DSP chips able to support multiple functions. This is due to continuous improvement in manufacturing techniques for creating chip components at extremely small sizes (fractions of a micron), therefore producing DSP chips with more built-in functionality. SDR devices will take advantage of these advanced DSP chips to have multiple functionalities such as supporting multiple access technologies (e.g., operate on different radio technologies). SDR devices are envisioned to interoperate with existing and evolving LMR systems by switching modes and also are capable of operating in multiple public safety frequency bands.

5.2 SDR Within LMR Networks

A public safety agency's ability to maintain seamless, reliable intra- and interagency communications is determined by its LMR system's architecture. Many federal agencies are in the process of transitioning from wideband analog systems to the Project 25-compliant narrowband digital trunked or conventional systems. The NTIA mandated this transition from wideband to narrowband operation, and the transition must be completed for VHF channels by 2005 and by 2008 for UHF channels. Similarly, many state and local governments are transitioning to narrowband systems but are more often considering 800 MHz trunked systems to replace their legacy systems. This strategy creates significant challenges in terms of interoperability for special and unique operational requirements. It is anticipated that SDR subscriber equipment will include the capability to operate across multiple frequency bands and technologies, providing interoperable communications between disparate networks. Figure 3 presents a general depiction of how SDR subscriber equipment will operate within public safety LMR networks.

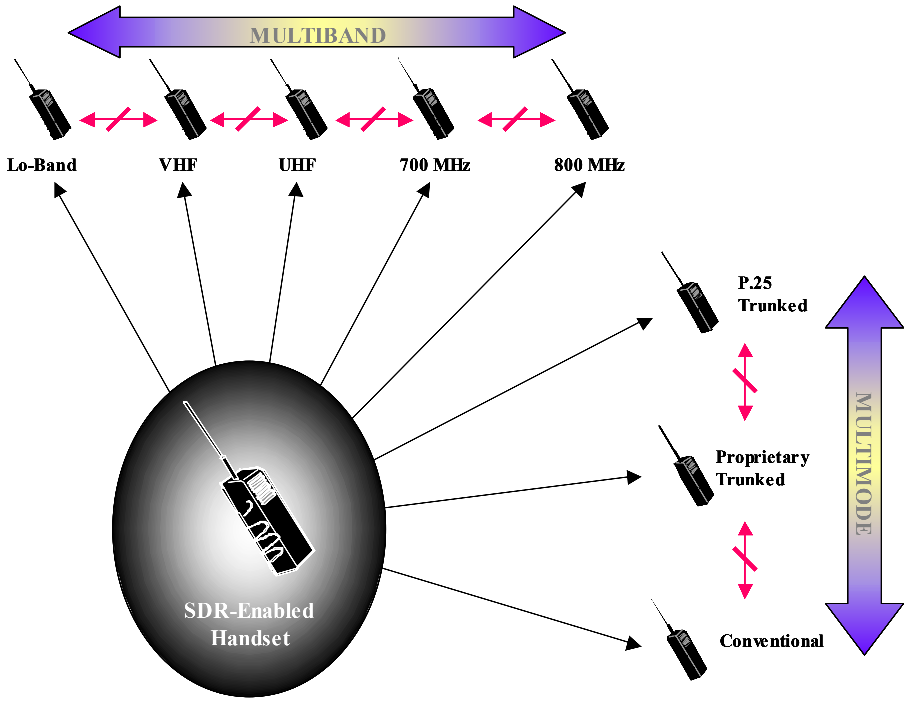


Figure 3
SDR–LMR Subscriber Terminal Equipment

5.3 SDR Technology Background

The Department of Defense (DoD) began the development of SDR technology through the SPEAKeasy research program in 1992. The objectives of the program were to consolidate a family of discrete military radios into a single platform using software radio technology. The SPEAKeasy program yielded significant advancements for SDRs. The program proved the feasibility of SDR technology, achieved a significant reduction in the size and weight of SDR devices, and increased both computational capacity and overall system performance.

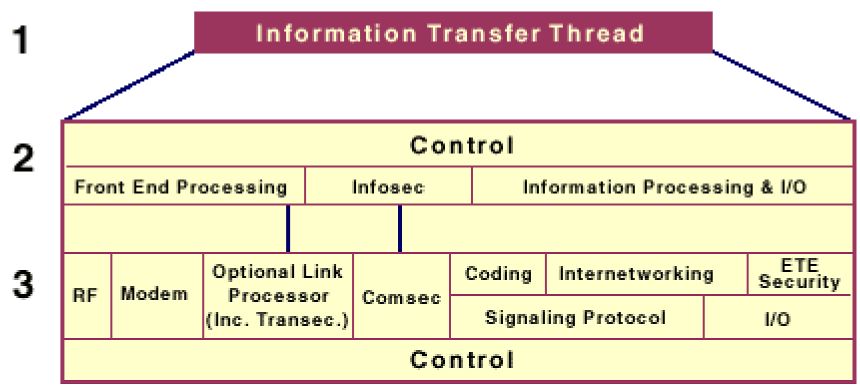
In 1996, the U.S. Government invited industry to participate in the Modular Multifunction Information Transfer Systems (MMITS) forum. This forum initially functioned as a guiding body for the establishment of open architecture standards for the SPEAKeasy program. The MMITS forum eventually shifted its focus from the government community to the commercial community. In 1999, the MMITS forum officially changed its name to the SDR Forum. Since then, the SDR Forum has promoted SDR technologies with applications for commercial cellular, Personal Communication Systems (PCS), and emerging third-generation (3G) and fourth-generation (4G) cellular services.

The Joint Tactical Radio System (JTRS), a DoD research program, has performed extensive research in the area of SDR technology. The mission of the JTRS effort is to develop a family of tactical software radios, all built on a common, open software communications architecture (SCA). The SDR Forum has adopted the SCA standard for developing commercial SDR products.

5.4 SDR Architecture

The generic SDR architecture[6] comprises specific functional blocks connected via open interface standards. The SDR architecture supports three specific domains: hand-held, mobile, and base-station (or fixed site). For the purposes of this assessment, only the architectures for hand-held and mobile SDR devices will be identified. The software is implemented by controlling the characteristics of equipment/device subsystems that support scaleability and flexible extensions of applications. Modularity is an important factor in the implementation of software applications within open systems.

Figure 4 illustrates a high-level hierarchical functional model for a two-way (send and receive) SDR device. Three views of increasing complexity are presented. The top-level view is a simple representation of an entire information transfer thread. The left side interface is the air interface. The right side interface is the user interface. The next level view identifies a fundamental ordered functional flow of four significant and necessary functional areas; (1) front end processing, (2) information security, (3) information processing, and (4) control.



source: SDR Forum

Figure 4
Hierarchical Functional Model of SDR

- Front end processing consists of the physical air (or propagation medium) interface, the front-end radio frequency processing, and any frequency up and down conversion. Also, modulation/demodulation processing is contained in this functional block area.

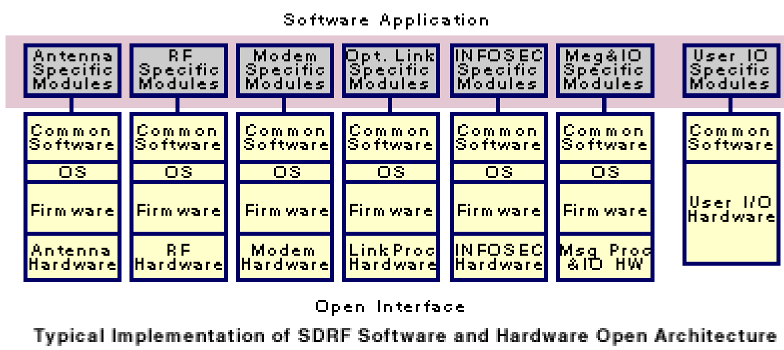
- INFOSEC provides user privacy, authentication, and information protection. In the military and, subsequently, public safety communities, INFOSEC for sensitive and classified communications must be consistent with the government security policies as defined by the NSA.

- Content or information processing is the decomposition or recovery of the imbedded information containing data, control, and timing. Content processing and I/O

[6] *This discussion of SDR architecture is adapted from the SDR Forum's "SDR Primer" - http://www.sdrforum.org/sdr_primer.html*

functions map into path selection (including bridging, routing, and gateway), multiplexing, source coding (including vocoding, and video compression/expansion), signaling protocol, and I/O functions.

The functional components of SDR architecture are connected together via open interfaces. Each functional component in the SDR architecture is controlled with software. The software necessary to operate an SDR device is called a software application. Figure 5 illustrates the SDRF (Software Defined Radio Forum) open architecture comprising of seven independent subsystems interconnected by open interfaces. Interfaces exist for linking software application specific modules into each subsystem. Each subsystem contains hardware, firmware, an operating system, and software modules that may be common to more than one application. The application layer is modular, flexible, and software specific. The common software Application Programming Interface (API) layer, is typically standardized with common functions based on defined interfaces.



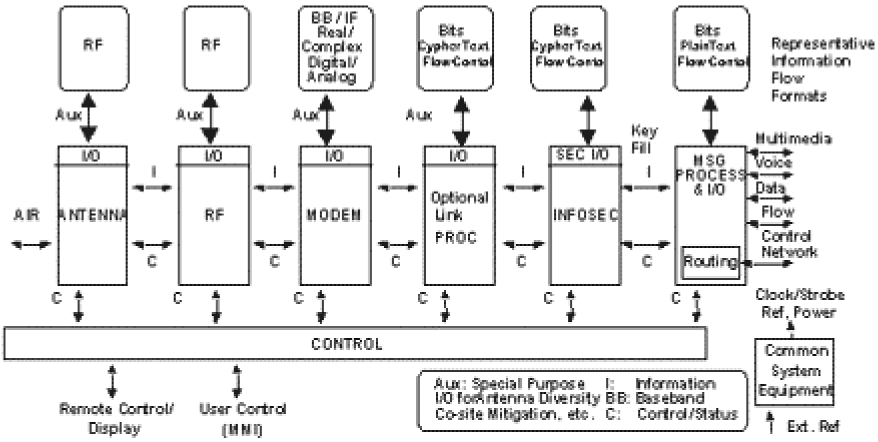
source: SDR Forum

Figure 5
Generic Software Subsystem SDR Model

5.5 SDR Functional Perspective

Figure 6 illustrates the SDRF functional interface diagram and demonstrates how the SDRF Architecture provides definition to the functional interfaces[7]. A representative information flow format is provided at the top of the diagram. For example, information transfer is effected throughout the functional flow within the SDRF architecture to/from antenna-RF, RF-modem, modem-INFOSEC, and INFOSEC-Message Processing interfaces. The specific implementation would determine the actual control and status between the interfaces and functional module.

[7] *This discussion of SDR Functional Perspective is adapted from the SDR Forum's "SDR Primer" - http://www.sdrforum.org/sdr_primer.html*

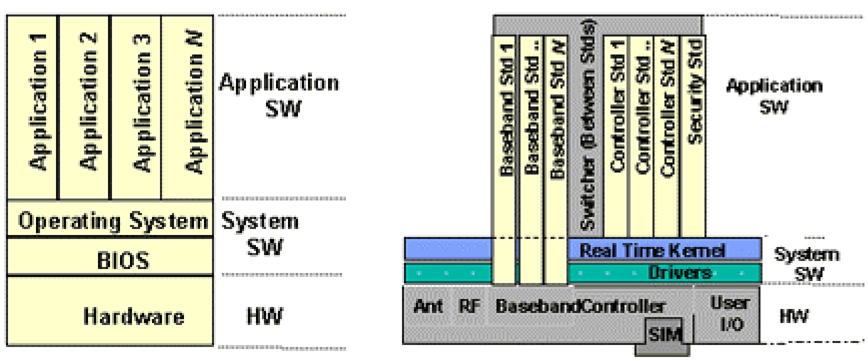


source: SDR Forum

Figure 6
Functional Subsystem SDR Model

The actual information being transmitted by an SDR device follows the paths illustrated by the "I" within Figure 6. The SDR device operates by providing control ("C") messages through each of the functional blocks as indicated by the Control function. As an example, the frequency at which a wireless signal is generated is determined by frequency generation in the RF function. Through the control capability, an SDR device would allow this frequency to be changed to accommodate different operating environments (useful in situations where users move between systems with different operating frequencies).

An example SDR implementation for a piece of subscriber equipment may be viewed in comparison with a generic PC model in the form of a multiple service model as illustrated below in Figure 7.



Generic PC HW/SW Architecture

Handheld Multiple Service Model Using SDR

source: SDR Forum

Figure 7
Functional Software Subsystem SDR Model

The specific implementations for each service (e.g., different air interface technologies in communication systems) are shown to be included through the system software layer and directly interfacing the hardware layer. The most common factors considered in SDR subscriber equipment development are based upon the following: battery power, size, weight, and specific user and cost requirements. In order to achieve processing speed and efficiency, the majority of implementations are programmed very close to the underlying hardware or logic, using low-level languages such as assembly language. The task of switching between multiple operating bands using the same or different RF hardware is managed by a combination of the service switcher and the controller services for each individual operational mode.

5.6 Advancement of SDR Technology

Radio technology has progressed from being hardware dependent to being more software oriented. Many view SDR as the next logical step in the evolution process of radio technology. Figure 3 shows the evolution of SDR technology. The evolution of all radio technologies begins with hardware radios. Between now and roughly 2008, software defined radios will start to become more available. In the future, SDRs will be deployed offering more flexibility and more capabilities. Much farther in the future, the ideal SDR device will become available, offering the most flexibility and the most capabilities. The following paragraphs describe the four phases of radio development shown in Figure 8.

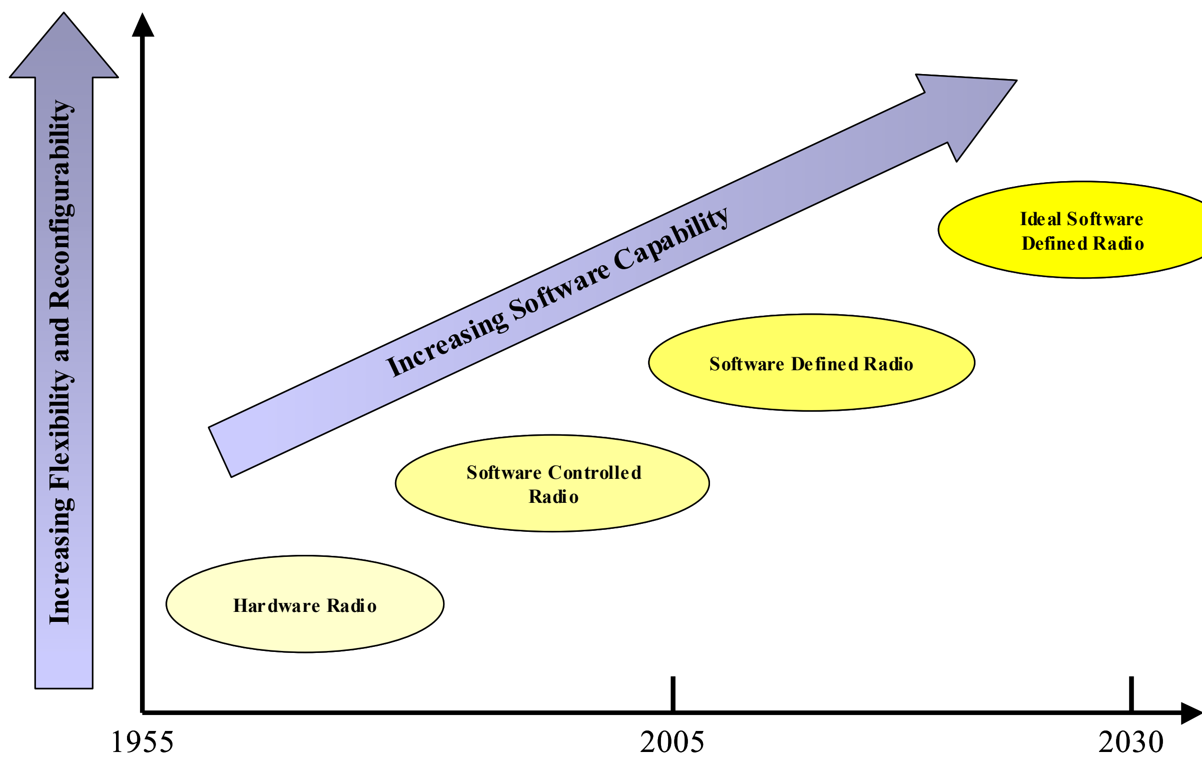


Figure 8
SDR Technology Advancement Path

- **Hardware Radio**—Hardware radios are the baseline for comparison with other radio technologies. Hardware radios were most commonly used in the 1950s and 1960s.

These radios were heavy but extremely durable and long lasting. All radio components were hard-wired. Switches, dials, and buttons were the only means for a user to operate the radios. Any changes in operating frequency required physically swapping the crystals that defined the operating frequency of the radio. Typical examples are Bendix King, General Electric, and Motorola radios.

- **Software Controlled Radio**—These radios are implemented using modern digital semiconductor technology. The digital integrated circuitry (IC) inside software controlled radios allows for the limited control of functions to be implemented by software. Examples of these control functionalities include frequency reprogramming, changing encryption keys, and programmable switches and buttons. However, software controlled radios cannot change modulation types or operating frequency bands. Most modern LMR radios available today can be classified as software controlled radios.

- **Software Defined Radio**—The majority of the components in an SDR device are implemented by software. SDR differs from software controlled radio in that DSP chips are used to generate various modulation types, filters, and air interfaces. However, the RF front end of SDR is still implemented by analog circuitry, which often leads to bulky design, multiple antennas, and architecture complexity.

- **Ideal Software Defined Radio**—Ideal SDRs differs from SDRs in that all radio components will be implemented by software, including the RF front end. It is expected that ideal SDRs will have a dramatic improvement in overall system performance relative to the initial generations SDRs. However, because of technology limitations, ideal SDRs are unachievable today and may not be realizable in the foreseeable future.

6. CONCLUSION

Although the SDR technological advances are promising, SDR technology suitable for use by the public safety community is still in an early stage. This is due to several factors. SDR technology has the potential to cause interference with other existing radio systems. The FCC has made rulings addressing interference issues but has not yet completely addressed other concerns such as spectrum management. Another factor that indicates that the development of SDR technology is in its early stages is that the traditional LMR equipment vendors, although active in the development of SDR technology, have neither invested substantial resources nor given formal timelines for the development SDR products.

As the SDR technology matures, the public safety community can gain many benefits. The most important benefit will be interoperability across dissimilar radio networks, frequency bands, and technologies. Other benefits that SDR technology could provide the public safety community include enhanced capabilities such as data communications and improved user-friendly operation of subscriber equipment.

It is important for the public safety community to take note of the challenges that may be introduced with SDR technology. The most significant and pervasive challenge will be mitigating potential interference that SDR devices may have with other radio systems. The FCC's ruling of September 12, 2001, addresses this interference issue by requiring SDR developers to provide extensive test data to prove that interference is minimized.

Many possibilities exist for a wide-range of SDR-based services and applications for use within the military, commercial, and public safety communities. The SDR services and applications being considered today are small subsets of what could be offered in the future. The military community has taken the first steps in implementing an SDR test-bed; eventually the commercial community will develop innovative features and services that will support the wide-scale acceptance of SDR technology. The public safety community can leverage lessons learned from those prior efforts to help create SDR devices that will improve radio communications and increase interoperability, enhancing the ability of public safety agencies to achieve their mission of protecting lives and property.

APPENDIX A—ACRONYMS

APPENDIX A—LIST OF ACRONYMS

3G	Third Generation
4G	Fourth Generation
API	Application Programming Interface
CDPD	Cellular Digital Packet Data
DES	Digital Encryption Standard
DoD	Department of Defense
DSP	Digital Signal Processing
FCC	Federal Communications Commission
I/O	Input/Output
IC	Integrated Circuit
IN	Intelligent Network
INFOSEC	Information Security
IV&D	Integrated Voice and Data
JTRS	Joint Tactical Radio System
LMR	Land Mobile Radio
MExE	Mobile Execution Environment
MHz	Megahertz
MMITS	Modular Multifunction Information Transfer Systems
NCIC	National Crime Information Center
NSA	National Security Agency
NTIA	National Telecommunications and Information Administration
OTAR	Over-the-Air Rekeying
PCS	Personal Communication System
PSWN	Public Safety Wireless Network
RF	Radio Frequency
RFI	Request for Information
SCA	Software Communications Architecture
SDR	Software Defined Radio
SDRF	Software Defined Radio Forum
VHF	Very High Frequency
WAP	Wireless Application Protocol
WINS	Wireless Interoperable Network Strategy

APPENDIX B—SDR FORUM MEMBERSHIP

APPENDIX B—SDR FORUM MEMBERSHIP

SDR Forum Member	Location	Telephone Number
3e Technologies Intl. Inc.	Rockville, MD	(301) 670-6779
The Aerospace Corporation	El Segundo, CA	(310) 336-5000
AirNet Communication Corporation	Melbourne, FL	(321) 984-1990
Airvana	Chelmsford, MA	(866) 344-7437
Altera	San Jose, CA 95134	(408) 544-7000
Applied Physics Lab (JHU)	Laurel, MD	(240) 228-5000
Assurance Technology	Carlisle, MA	(978) 369-8848
Boeing	Chicago, IL	(312) 544-2000
CCL/Industrial Technology Research Institute	Hsinchu, Taiwan	
Center for Wireless Communications, National University of Singapore	Singapore Science Park II, Singapore	(65) 872-9030
Chunghwa Telecom Labs	Taiwan	886 + 2 + 2326-2475
Cingular Wireless	Atlanta, GA	1-866-CINGULAR
Communications Research Centre Canada	Ottawa, ON Canada	(613) 991-3313
Com-Net Ericsson	Lynchburg, VA	(804) 385-2329
Defence Evaluation & Research Agency	Hants GU14 OLX, United Kingdom	+44 (0)1252 393300
Defence Science and Technology Organisation, Australia (DSTO)	Australia	(02) 6265 9111
Digital Transit	Mountain View, CA	(650) 230-2600
Ditrans	Irvine, CA	(949) 453-0588
DND/DREO (Department of National Defence/Defense Research Establishment Ottawa)	Ottawa, Ontario	(613) 998-2203
DENSO Corporation	Long Beach, CA	(888) 96-DENSO
DSO National Laboratories	20 Science Park Drive, Singapore	(65) 776- 2255
EF Johnson Company (a Subsidiary of Transcrypt International, Inc.)	Washington, DC	(202) 833-7553
EnVia	San Jose, CA	(408) 777 4802
ETRI, Korea	Korea	(82) 42-860-6114
France Telecom		
Fujitsu	San Jose, CA	(408)-432-1300
General Dynamics	Falls Church, VA	(877) 449-0600
Global Communications Devices	North Andover, MA	(978) 685-6100
Harris Corporation	Melbourne, FL	(321) 727-9100
Helicon Networks	Seattle, WA	(206) 628-9140
Hitachi Kokusai Electric	San Jose, CA	(408) 456-2750
Huneed Technologies		
HW Communications	Lancaster, England	+44 (0) 1524 849196
HYPRES	Elmsford, NY	(914) 592-1190
IIT Research Institute	McLean, VA	(703) 918-4497

SDR Forum Member	Location	Telephone Number
Innovative Concepts	McLean, VA	(703) 893-2007
Intel	Chandler, AZ	(480) 554-8080
Intelectron	United Kingdom	01438 351313
Interactive Circuits and Systems	Ontario, Canada	(613) 749-9241
Isaac Newton Technologies		
ITT Industries	White Plains, NY	(914) 641-2000
Kenwood	Finksburg, MD	(410) 840-8784
Korea Electronics Technology Institute	Kyeonggi-Do, Korea	+82-31-6104-11
Litton/TASC	Arlington, VA	(703) 558-7400
Marconi Mobile	Chelmsford, Essex United Kingdom	01245 275299
Matsushita Europe	Holzkirchen, Germany	+49 (0) 8024 648-0
Mercury Computer	Chelmsford, MA	(978) 256-1300
The MITRE Corporation	McLean, VA	(703) 883-6000
Mitsubishi Electric	Cypress, CA	(714) 220-2500
Mnemonics	Melbourne, FL	(800) 842-5333
Mobilian	Hillsboro, OR	(888) 314-3606
Morpho Technologies	Irvine, CA	(949) 47-0626
Motorola, Inc.	Hanover, MD	(877) 873-4668
NASA Glenn Research Center	Cleveland, OH	(216) 433-4000
NTT	Tokyo, Japan	
NTT DoCoMo	Tokyo, Japan	
Orange PCS	Co. Dublin, Ireland	+353 1 289 1800
PAR—Rome Research Corporation	New Hartford, NY	(315) 738-0600
Peter G. Cook Consultancy	Mesa, AZ	(480) 733-8225
Quicksilver Technology	San Jose, CA	(408) 574-3351
Radio Research Laboratory		
Radreal Ltd		
RadioScape	Redwood City, CA	(650) 632-4514
Raytheon Systems	Lexington, MA	(781) 862-6600
Samuel Neaman Institute (Technion)	Israel	04-8320664 / 8293863
Samsung Advanced Institute of Technology	Korea	+82.331.280.8157
Samsung Yokohama Research Institute		045-510-3331
Sangikyo		
Sarnoff Corporation	Princeton, NJ	(609) 734-2000
Sasken Communication Technologies Ltd.	Bangalore, India	+91 80 528 1461
Seoul National University	Seoul, Korea	+82 2 880 5114
Sharp Corporation	Mahwah, NJ	(201) 529-8200
Siemens AG	New York, NY	1-800 - S I E M E N S
Sirific	Ontario, Canada	(519) 747-2292
Sirius Communications NV	Leuven, Belgium	+32 16 44 44 02
Siroyan Ltd	Berkshire, United Kingdom	44 (0) 118 949-7028
SK Telecom	Korea	82 2 2121 4717
Sonera	Washington, DC	(202)- 454 1900
Sony Computer Science Lab	Tokyo, Japan	+81-3-5448-4380
Southwestern Bell Technology Resources		

SDR Forum Member	Location	Telephone Number
Space Coast Communication Systems	Melbourne, FL	(321) 591-6199
SPAWAR Systems Center	North Charleston, SC	(843) 218-4000
Spectrum Signal Processing	Landover, MD	(301) 459-8888
Spinnaker LLC	Laguna Hills, CA	(800) 544-9885
Sprint PCS	London, KY	(888) 253-1315
Swedish Defense Research Agency	Sweden	+46 (0) 55 50 3000
TDK Electronics Ireland	Dublin, Ireland	01-4133200
Telecom Engineering Center	New Delhi, India	91-11-3326029
Telcordia	Morristown, NJ	(973) 829-2000
Thales/Racal Communication	Rockville, MD	(301) 208-7654
Tokyo Institute of Technology	Meguro-ku, Tokyo 152-8550	+81-3-5734-2353
Toshiba Research, Europe		
TRW	Cleveland, OH	
University of Karlsruhe	Karlsruhe	+49 7 21 6 08 - 43 40 - 60 97
U.S. Air Force Research Laboratory	Rome, NY	(315) 330-3053
Vanu, Inc.	Cambridge, MA	(617) 864-1711
Vertex Standard	Somerset, NJ	(732) 563-0366
Voicestream	Bellevue, WA	(800) 318-9270
Wireless Online	Santa Clara, CA	(408) 567-6600
Yokohama National University	Yokohama, Japan	045-339-3804
Yokosuka ITS Research Center	Japan	+81-468-47-5015

APPENDIX C—PROJECTED USER REQUIREMENTS

APPENDIX C—PROJECTED USER REQUIREMENTS

Software-defined radio (SDR) technology suitable for use by the public safety community is still in its infancy. As the technology matures, a more detailed understanding of how best to apply it to public safety requirements should emerge. When the time comes for the public safety community to elect to use the technology, a thorough requirements analysis must be conducted prior to SDR implementation in the public safety environment. The following are a sample of suggested user requirements for use in ensuring that the SDR subscriber equipment being considered actually has operational capabilities in the multitude of public safety radio environments.

C.1 Operational Uses

The SDR-enabled devices must allow public safety personnel to perform the following functions:

Suggested Overall Uses	
a.	Communicating among members of a specified work group within an agency
b.	Communicating among members of a specified work group composed of multiple public safety agencies with disparate radio systems
c.	Communicating among members of an interoperability work group(s) composed of multiple law enforcement, fire, and emergency medical response officials from state, local, and other federal agencies
d.	Broadcasting requests for emergency assistance to a specified group(s)
e.	Communicating with a designated dispatch center(s)
f.	Facilitating administrative functions with personnel outside of an agent’s own organization including state, local, and other federal agencies
g.	Functioning as a “cross-over” mobile data computing device

C.2 Features/Capabilities

The following features and capabilities are required for one or more of the required functions identified in D.1, Overall Uses.

Features and Capabilities	
a.	One-to-many communication
b.	One-to-one communication
c.	Unit-to-unit communication independent of the network infrastructure
d.	Transmit and receive from a handheld device
e.	Transmit and receive from inside designated buildings and facilities
f.	Maintenance of officer-to-officer communications when one or more officers leave their home radio system
g.	Place and receive an emergency call
h.	Place and receive an emergency alarm
i.	Simple to use, easy to operate, and easy to learn
j.	Secure communications capabilities
k.	Change encryption keys over the-air
l.	Support of wireless data applications, including crime database queries, transmission of fingerprints and mug shots, terminal-to-terminal messaging, telemedicine and telemetry data, and report writing

C.3 Technical Guidelines

These technical guidelines identify specific considerations that SDR subscriber equipment must meet.

Technical Guidelines	
a.	SDR subscriber equipment must be interoperable: 1. Allows users to communicate outside of their regularly designated radio system 2. Allows users to communicate in other radio system environments
b.	SDR subscriber equipment shall, at minimum, communicate with legacy, conventional, proprietary trunked, and Project 25 conventional and trunked systems
c.	SDR subscriber equipment shall operate in low-band, very high frequency, ultra high frequency, 800 megahertz (MHz), as well as the 700 MHz bands newly assigned to public safety
d.	SDR equipment shall be capable of operating in simplex mode, or unit-to-unit direct communications without accessing system infrastructure
e.	Local operational requirements surveys will determine specific geographic coverage areas. However, in general— 1. Portable coverage (via handheld device) will be required in metropolitan, border, campus, and designated buildings 2. Mobile coverage (via vehicle installed devices) will be required in interstate, rural, and Native American areas
f.	SDR subscriber equipment shall have the ability to establish temporary, deployable communications infrastructure
g.	SDR subscriber shall support common encryption algorithms, including digital voice protection, data encryption standard (DES), DES-XL, and Project 25 compliant DES output feedback, Advanced Encryption Standard, and Type I
h.	Key management shall support, at minimum, manual loading with the use of a key variable loader (KVL) and by over-the-air rekeying (OTAR)
i.	SDR subscriber devices shall provide integrated voice and data (IV&D) capability and be compliant with Project 25 data requirements