Requirements for Radio Software Download for RF Reconfiguration

SDRF-02-S-007-V1.0.0

(Formerly SDRF-02-A-0007-V0.0)

13 November 2002

Table of Contents

Preface

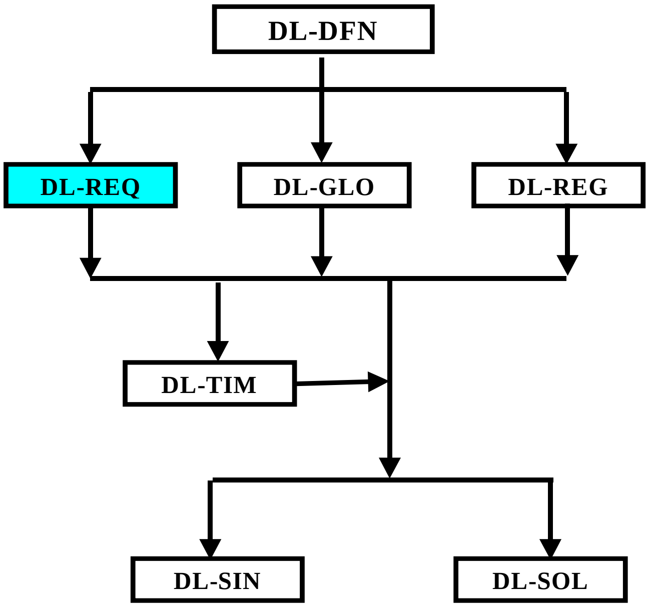
This document presents specific requirements for protocols for downloading software to a software-defined radio (SDR) device for its reconfiguration. The SDR device could be a small handheld communication device such as a cell phone, a slightly larger wearable device such as a manpack, or an immobile networked device such as a wireless base station. The requirements specified in this document have purposely been made general enough to encompass software downloads to all of the above types of SDR devices.

This document is Version 1.0 – it is the intent of the SDR Forum to seek inputs from relevant other organizations for consideration for Version 2.0 and later versions of this document.

This document is one document in a series of SDR Forum documents on radio software download[1]. The otherdocuments in this series are:

♦ DL-DFN:	Overview and Definition of Software Download for RF Reconfiguration
♦ DL-GLO:	Report on Global Radio Technology Development Organization Perspectives on Software Download for RF Reconfiguration
♦ DL-REG:	Report on Global Regulatory Views on SDR and Radio Software Download for RF Reconfiguration
♦ DL-TIM:	Timelines for Software Download for RF Reconfiguration
♦ DL-SIN:	Software Download for RF Reconfiguration Security and Integrity
♦ DL-SOL:	Specifications of Common Solutions for Software Download for RF Reconfiguration

The relationship of these documents is seen in the figure below. DL-DFN is the overarching document that provides a foundation for the remaining documents and drives the development of the other documents. Documents DL-TIM, DL-REQ, DL-GLO, and DL-REG are parallel documents that provide the basis for further work in DL-SIN and DL-SOL. It is these latter two documents that are the ultimate goals of this series of SDR Forum documents on software download. As work on these documents progresses, certain documents such as DL-SIN and DL-SOL may be combined into a single document.



Relationship of SDR Forum Software Download Documents

[1] This series of documents utilizes and extends the work of earlier SDR Forum publications including the SDR Forum Technical Report 2.1, "Architecture and Elements of Software Defined Radio Systems as Related to Standards."

Requirements for Radio Software Download for RF Reconfiguration

1 Introduction

This document presents specific requirements for radio software download (i.e., the downloading of software for RF reconfiguration) in the context of a software-defined radio (SDR) device. In many cases provisions for radio software are also applicable to applications (non-radio software) running on the system. When applicable, this document also indicates download considerations for application software.

The SDR device could be a small handheld communication device such as a cell phone, a slightly larger wearable device such as a manpack, or an immobile networked device such as a wireless base station. The requirements specified in this document have purposely been made general enough to encompass radio software downloads to all of the above types of SDR devices.

A companion document to this document, "Overview and Definition of Software Download for RF Reconfiguration" (DL-DFN), defines radio software download as the process of delivering reconfiguration data and/or new executable code to an SDR device to modify its operation or performance. This definition makes a distinction between radio software download and non-radio software download (with examples of the latter including a wide variety of subscription or free news and information, proprietary corporate data, email, and multimedia material such as MP3 files[2]).

This document is focused primarily on high-level functional requirements for software download for RF reconfiguration. It does not describe mechanisms to satisfy these requirements, i.e., the requirements described herein are not detailed design requirements.

Rather than attempting to cover all military, civil, and commercial requirements, a comprehensive list of general requirements is proposed. Specific sets of requirements for the commercial, civil, and military sectors may be derived as subsets of this comprehensive list.

This document is organized as follows. Section 2 discusses general technical requirements from the point of view of the user, operator, and manufacturer. This section also provides regulatory considerations that need to be taken into account regarding radio software download. Section 3 provides an overview of the radio software download process with a brief description of each of its steps, such as initiation, mutual authentication, authorization, installation, and so on. Section 4 provides the detailed technical requirements for radio software download. This section is divided into four major parts. Section 4.1 provides requirements for each step of the radio software download process, Section 4.2 provides requirements for the SDR device that support radio software downloads, Section 4.3 provides requirements for the network that supports radio

[2] There are authentication and authorization mechanisms that have already been developed for non-radio or content information software download that may have applicability to radio software download as well.

software downloads, and Section 4.4 gives brief overview of security issues related to radio software download. Finally, Section 5 provides a summary of all the requirements specified in this document.

2 General Technical Requirements

This section provides general technical requirements from the points of view of users, operators and manufacturers. More specific technical requirements that incorporate these requirements from different viewpoints are found in Section 4 of this report.

2.1 User Requirements

Users primarily are interested in having flexible terminals that have access to third party software. They are also concerned about security and privacy, the length of time it takes to perform a download, and download costs. Users, in general, do not care about technology. Therefore, manufacturers, network operators, and service providers act as proxies for users to ensure that user requirements are met.

User requirements include:

- Convenience of operation
- Provision for security and privacy
- Understanding of service charges being incurred, both for application use and download
- Ability to add new services and functions
- Reliable operation

2.2 Operator Requirements

Operators and/or service providers use network infrastructure and radio resources (spectrum) to provide services to end users. With the advent of radio software download and reconfigurable SDR devices, operators can use the resulting flexibility to provide better services to end users, configure and provision network infrastructure more efficiently, fix bugs and upgrade radios to newer technologies more efficiently, and make better use of existing radio resources. In addition, operators are concerned about any potential sources of interference in their networks because interference can adversely affect the service quality that is perceived by the end users as well as the number of users or amount of traffic that can be carried by the operator's network. Finally, security of the network and protection of software and data are very important to operators.

These high-level operator considerations thus require that radio software download provide for:

- Remote "bug fixes" and download of new versions of radio software to either specific SDR devices or a wide range of SDR devices deployed in the network
- Remote reconfiguration of SDR base stations to meet changing demands on the network
- Protection against unintentional or malicious radiation of signals having power, frequency and modulation combinations that are not authorized for use in the operator's network.
- Assurance that reconfigured SDR devices must not inadvertently cause interference in the network (many of the regulatory considerations discussed in section 2.4 are concerns for the operator as well)

- Authentication of parties involved in the radio software download
- Verification that the party requesting the radio software download is authorized to do so
- The integrity of the downloaded or user data must always be assured and verified. The most secure method is via cryptographic encapsulation.
- Confidentiality of the downloaded or user data may optionally be assured by encryption.
- Capabilities exchange between the network and SDR device, as well as between the SDR devices of two subscribers (this may be especially required for security related applications).
- Considerations of download time and radio resources required for the radio software download
- Customized features or services, either via original equipment manufacturer or third party vendor
- Maintainance of a dynamic database of most current configurations of SDR devices deployed in the network
- Software download mechanisms that work for a variety of types[3] of software download including:
    - Primary radio software (e.g. patches for bug fixes, new air interface, etc.)
    - Ancillary radio software (e.g., radio software that may affect the control functions of the SDR device, new user interface, I/O drivers, etc.)
    - Non-radio software (e.g., user applications)
    - Download of only a few reconfiguration parameters that cause the SDR device to configure itself according to the values specified by these parameters.
- Control of the software download process.

2.3 Manufacturer Requirements

Manufacturers requirements stem from a business-case need to be able to perform the following functions via download to SDR-capable devices:

- Software “bug fixes”
- Addition of new capabilities to the device

Manufacturers desire “agnostic” (i.e., technology neutral) standards that will permit the accomplishment of the above functions across a wide variety of SDR-capable platforms (i.e., across many different terminals, base stations, and mobile devices). To the extent possible, the download architecture and protocols should be interoperable for these devices.

High-level download considerations from a manufacturers point of view include:

- Platform-independent protocols to deliver software from its source to target systems
- The ability to reconfigure FPGAs
- Incremental software download to avoid complete download of entire software suite
- Complexity of the download process

[3] Definitions for radio software download and the characterizations of software download as defined by the SDR Forum may be found in Reference [1].

- Download time and power consumption
- Memory requirements and memory management to support download
- Liability for the download software
- Authorization for downloaded software should be by arrangement (financial, support, etc.) between the SDR device owner and the software manufacturer/provider.
- Responsibility for maintenance
- Download processes that include protection provisions acceptable globally by regulatory authorities
- Protection against unintentional or malicious radiation of signals having power, frequency and modulation combinations that are not consistent with the manufacturer's conformance declaration, type acceptance, etc.

From the perspective of manufacturers (most of which are international companies that provide equipment in all regions of the world), the global aspect of radio software download must be considered from both technical and regulatory points of view.

2.4 Regulatory Considerations

The basic concern of regulators is to ensure that SDR operations are limited to those frequency bands, output power and transmitted signal characteristics that have been authorized. There is, of course, no single global regulatory entity for wireless devices, and therefore it important in defining standards to recognize that there are differences in security policies among different global regulatory authorities. Nevertheless, it is to the benefit of all actors in the wireless field (end users, service providers, network operators, and manufacturers) for industry to develop technical requirements that are sensitive to regulatory considerations. These considerations, while not adopted in international codes, nevertheless have a global commonality of purpose. In developing standards in this arena, the input of regulatory authorities around the globe is paramount so that their individual requirements can be given appropriate consideration.

High-level regulatory considerations include provisions for:

- Conformance to type approval for defined software/hardware combination for SDR-capable devices.

Protection against unintentional or malicious radiation of signals having power, frequency and modulation combinations that are not legally sanctioned.

- Identification and characterization of parameters that can be modified by downloaded software in SDR equipment.
- Appropriate type approval and configuration management for SDR equipment.

2.5 Other Considerations

The following items must also be considered regarding radio software download.

- *Malfunction Protection:* After the downloaded radio software has been installed on the SDR device, other changes could be made to the SDR device, potentially at some future date. Such changes may include the addition of other software modules, or an upgrade to the SDR device's operating system, etc. It must be ensured that any downloaded radio software installed on the SDR device does not malfunction or cause the SDR device to emit undesirable radio frequency waves when future changes are made to the SDR device's software. This requirement may make it necessary to have an agreement between the software vendor and the SDR device manufacturer to exchange information that would enable the software vendor to develop radio software that prevents undesirable operation.

- *Responsibility for Maintenance:* When a radio software module is downloaded and installed on an SDR device to enable or enhance its functionality, that radio software module becomes a part of the SDR device. However, there needs to be a clear agreement between the software vendor that developed the radio software module and the service provider, network operator, equipment manufacturer, etc. to determine who is responsible for issuing maintenance updates for that radio software module.

- *Billing, Licensing, and Ownership:* Clear agreements must be in place between the SDR device user, the service provider, network operator, equipment manufacturer, and software vendor regarding the licensing and ownership of a radio software module that is to be downloaded and installed by the user. These factors relating to SDR devices may be dynamic to the extent that they can change over time, as a function of physical locations and associated network connectivity, and service profiles. Billing arrangements must have been worked out to determine how, on what basis, and who should charge the user for downloading and installing the radio software module.

3 Overview of the Radio Software Download Process

Radio software download involves the transfer of software via:

- A remote server in which download is accomplished over-the-air via the actual radio interface through the supporting core network, or
- A local server that employs a variety of mechanisms (e.g., attached cable, infrared, Bluetooth, etc.), but does not involve the over-the-air interface.

This section presents an overview of the steps involved in the radio software download process, which can be divided into sets of Pre-, During-, and Post-Download steps, as described below.

Pre-Download (preparatory): These are events that lead to the download of software to the device. Such events are dependent upon the type of application and generate the decision to download. They include:

- Discovery of the need for download; i.e., the process by which a determination is made that there is a need for a software download
- Initiation of the download by the network, the user, or the application
- Download setup, such as determination of download process steps to be executed including their order, and determination of security mechanisms (for example encryption, integrity, authentication, etc.) to be used and portions of the download process to be protected
- Mutual authentication between the SDR device and the network from which software is to be downloaded

- Authorization to verify that the SDR device user has permission to receive, install, and utilize the radio software download
- A capability exchange, which may include user profile, SDR device capability, network compatibility, etc.
- Download acceptance exchange
- Determination of permissible access rights to proprietary software or private data while it is being downloaded to the SDR device

During-Download (procedural): Once the decision to download has been made, the events related to the download process begin. These events include:

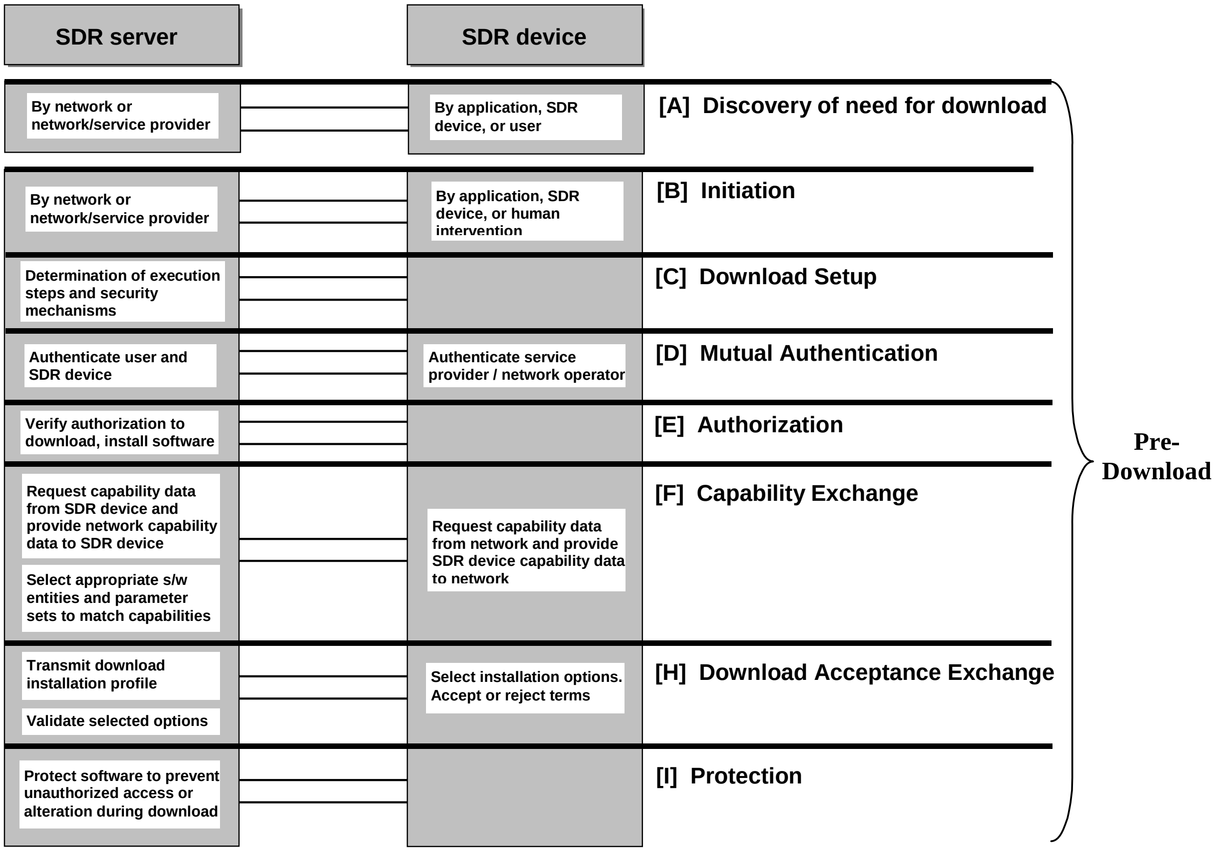
- Physical transfer of the software from the software server to the SDR device
- Verification of the integrity of the downloaded software with various methods such as
  - Cryptographic encapsulation of the downloaded software is the preferred method and may also be used to provide authentication of the sender
  - Cyclic Redundancy Code (CRC) checks can provide a check on integrity of the data but may be altered by a third party and does not provide authentication of the sender
- Retransmission requests
- Placement of downloaded software in secure local storage

Post-Download (installation): Once the actual software has been downloaded and verified for integrity, the following events may occur:

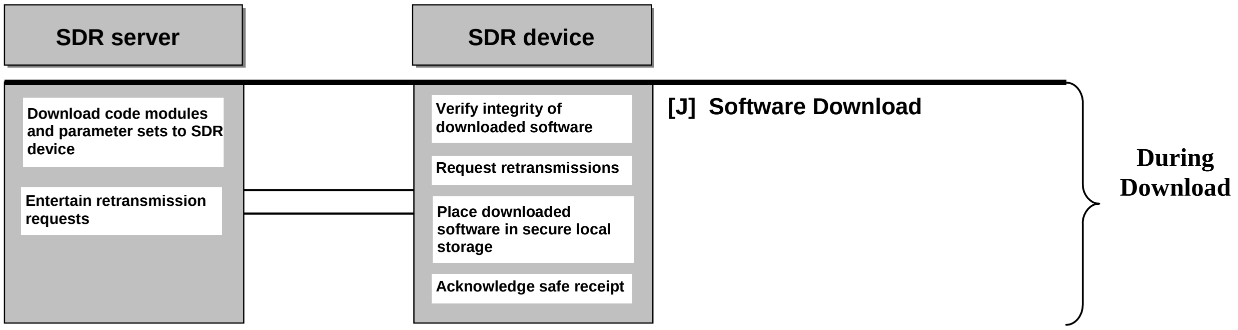
- Log transaction details via audit trail device
- Installation of the software
- Validation of the performance of the software, possibly by running certain critical functionality tests and reporting results back to the network (in-situ testing)
- Non-repudiation exchange
- Recovery efforts in the event that the downloaded software causes problems in the SDR device after being installed.
- SDR device reconfiguration
- Update of internal capability descriptors

Figure 1 gives a graphical overview of the radio software download process.

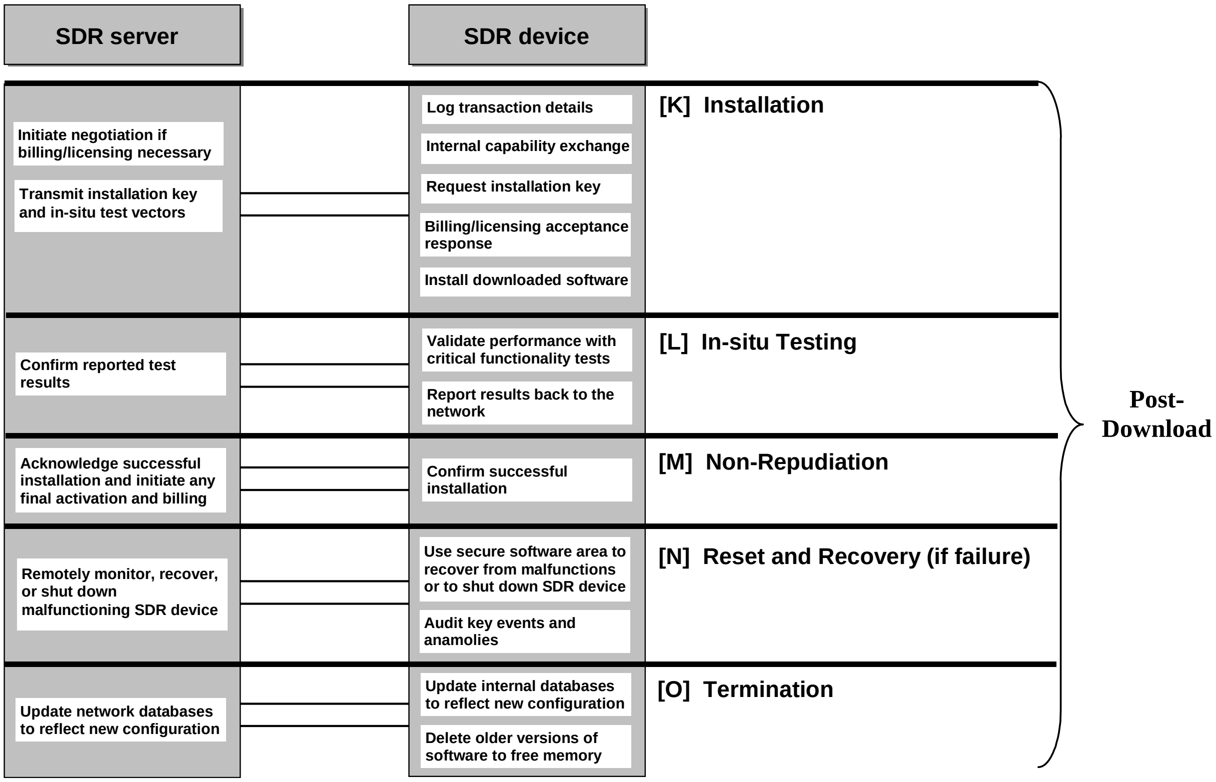
As the industry develops and refines this download process, it is appropriate to note that some parts of this process may be correctly seen as elements to be standardized whereas other parts of the process may be correctly seen as proprietary.


SDR server
SDR device
By network or network/service provider
By application, SDR device, or user
[A] Discovery of need for download
By network or network/service provider
By application, SDR device, or human intervention
[B] Initiation
Determination of execution steps and security mechanisms
[C] Download Setup
Authenticate user and SDR device
Authenticate service provider / network operator
[D] Mutual Authentication
Verify authorization to download, install software
[E] Authorization
Request capability data from SDR device and provide network capability data to SDR device
Select appropriate s/w entities and parameter sets to match capabilities
Request capability data from network and provide SDR device capability data to network
[F] Capability Exchange
Transmit download installation profile
Validate selected options
Select installation options. Accept or reject terms
[H] Download Acceptance Exchange
Protect software to prevent unauthorized access or alteration during download
[I] Protection
Pre-Download

Part (a) – Pre-Download (Steps A to I)


SDR server
SDR device
Download code modules and parameter sets to SDR device
Entertain retransmission requests
Verify integrity of downloaded software
Request retransmissions
Place downloaded software in secure local storage
Acknowledge safe receipt
[J] Software Download
During Download

Part (b) – During Download (Step J)


SDR server
SDR device
Log transaction details
Internal capability exchange
Initiate negotiation if billing/licensing necessary
Request installation key
Transmit installation key and in-situ test vectors
Billing/licensing acceptance response
Install downloaded software
[K] Installation
Validate performance with critical functionality tests
Confirm reported test results
Report results back to the network
[L] In-situ Testing
Acknowledge successful installation and initiate any final activation and billing
Confirm successful installation
[M] Non-Repudiation
Use secure software area to recover from malfunctions or to shut down SDR device
Remotely monitor, recover, or shut down malfunctioning SDR device
Audit key events and anamolies
[N] Reset and Recovery (if failure)
Update internal databases to reflect new configuration
Update network databases to reflect new configuration
Delete older versions of software to free memory
[O] Termination
Post-Download

Part (c) – Post-Download (Steps K to O)

Figure 1: Overview of the Radio Software Download Process

4 Specific Technical Requirements

This section provides a description of specific requirements that arise from the process steps outlined in Figure 1. These steps invoke both the SDR device and the SDR server. Therefore, following a description of download process requirements in section 4.1, specific requirements placed on the SDR device are discussed in section 4.2. Moreover, since many actors (e.g., regulators, operators, and manufacturers) have particular interest in over-the-air download, special attention must be given to the requirements placed on the wireless network. These requirements are discussed in section 4.3. Finally, section 4.4 gives a brief overview of security requirements for radio software download.

For near-term commercial SDR systems, subsets of the requirements discussed in this section may be derived, as applicable. This is required to enable near-term SDR systems to start implementing a subset of the download process and evolve gradually towards the full-fledged download process as SDR devices and network capabilities are enhanced. Similarly, subsets of requirements for civil and military SDR systems may also be derived as appropriate for the time frame of usage.

4.1 Download Process Requirements

The following subsections expand on the process flow provided in Figure 1.

4.1.1 Discovery of the Need for Download

This is the first step by which the need for radio software download is discovered. This discovery may be made by:

- ♦ *The Application* – An application operating over a wireless network may sense the availability of a newer version of software available in the network and may initiate the download process to upgrade its resident software.

- ♦ *The SDR Device* – The SDR device may monitor the network for the availability of new services or upgrades to software residing on the SDR device.

The Network – The network may monitor for SDR devices that should be updated to fix a bug in the existing software residing on the SDR device, to upgrade the SDR device’s existing software to a newer version, or to make the SDR device capable of newer services or applications. For security reasons it is desirable for the network to require permission from the SDR device before being able to “discover” SDR capabilities, software and versions.

- ♦ *The Network/Service Provider* – The network operator, service provider, or their agent, using mechanisms in the network, may discover the SDR devices whose existing software needs to be updated.

- ♦ *The User* – The end user may discover the need for a software download to access new functions or by recognizing the need for a new service capability.

Requirement: The radio software download process shall allow discovery of the need for radio software download to be made by the application, the SDR device, the network, the network/service provider, or the user.

4.1.2 Initiation of the Software Download Process

Initiation of the software download is subsequent to discovery of the need for a software download. Similar to “discovery,” “initiation” is a process that can be performed by:

- ♦ *The Application* – After discovery of the need for a software download, the initiation process for the application may include the following steps:

    - ▪ Decision as to whether the download should be initiated: The application may initiate action automatically or it may request a decision by the user as to whether or not the download should be initiated.

  - The application notifies the server if the decision is to initiate the download.

- *The SDR Device* – The SDR device schedules the initiation of the download process. This may be based on when operating conditions, such as quality of radio channel etc., are more suitable for the download.

The Network – The network schedules the initiation of the download process at an appropriate time based on operational criteria or network provider directions.

- *The Network/Service Provider* – The network provider, service provider, or their agent, may initiate the download process to push the software download to the SDR device.

- *Human Intervention by Device User or Technician* – The radio software download process may be initiated manually.

  - The SDR device user may initiate the process by connecting (through wireless or non-wireless means) to a network server.
  - A service technician may initiate the download process by plugging the SDR device into a cradle at a service location. This method of initiation is applicable in the case when the SDR device is a small handheld type of device.
  - A service technician may initiate the download process by establishing a communication link between the SDR device and a network server. This method of initiation is applicable when the SDR device is an immobile base station type of device deployed in the field.
  - Human intervention is required when the SDR device user requests a service that is not currently supported by the SDR device and requires the download of new software to the device in order to be supported. For example, a user may request packet data service in a voice-only capable SDR device. A reconfiguration management entity may then process the user's request and prompt the user to confirm the initiation of the download process. If the user provides a confirmation, the reconfiguration management entity may then initiate the download.

Requirement: The download process, SDR device, and network shall be capable of supporting download initiation by the application, the SDR device, the network, the network/service provider, or by human intervention (user or technician).

4.1.3 Download Setup

Depending upon the reason for the radio software download, some or all steps of the download process shown in Figure 1 may be executed. The decision regarding which steps need to be executed, and in which order, needs to be taken as soon as download is initiated and prior to the execution of any further steps in the download process. This is called Download Setup.

If the network already knows the capabilities of the SDR device due to a very recent capability exchange, it may wish to bypass the capability exchange step for better efficiency. The decision to bypass capability exchange is made in the Download Setup stage.

If the network simply wants to extract the detailed capability of the SDR device, the Download Setup may configure the download process to execute only steps D, E, and F, thus allowing a capability exchange to take place.

If new software needs to be downloaded to several SDR devices, but with a requirement that it must not be installed and configured before a certain date and time, the Download Setup may configure the download process to terminate after the completion of step J (Software Download) in Figure 1, and resume from step K onwards after a certain date and time.

An important decision that needs to be taken in the Download Setup stage is the determination of security mechanisms (for example encryption, integrity, authentication, etc.) to be used during the download and portions of the download process to be protected.

Requirement: The download process shall have the equivalent of a Download Setup stage, which decides, based on the reason for download, which steps in the download process need to be executed, with what security provisions, and in which order.

4.1.4 Mutual Authentication

Authentication is the ability to verify the origin of a piece of information, which, in the context of this document, is the radio software. Prior to the installation of any newly downloaded software, an SDR device must be able to verify that the software originated from a trusted server. It is crucial to perform authentication of the various parties involved in the download process to prevent any fraudulent use, fraudulent intercept, or denial of service attacks that affect the radio software download or the SDR device.

User authentication needs to be performed to verify the identity of the SDR device user and prevent unauthorized user access. This authentication may be done by using a Subscriber Identity Module (SIM) card, by cross-referencing the terminal serial number with the subscriber database, or similar methods.

There needs to be an authentication of the identities of the SDR device (hardware and software). The hardware authentication may be done by querying the SDR device for its International Mobile Equipment Identity (IMEI), Electronic Serial Number (ESN), or similar methods. The software authentication may be done by digital signatures, or other suitable methods.

The identity of the service provider or network operator also needs to be verified by the SDR device in order to prevent unauthorized network operators from conducting download transactions with SDR devices. These types of authentication operations may be done using public key cryptography methods, digital signatures, or other such suitable methods.

Requirement: The download process shall employ a rigorous mutual authentication procedure for validating the identities of the SDR device (hardware and software), the user, the service provider, the network operator, the manufacturer, and the regulatory organization, prior to allowing the download of radio software to the SDR device.

4.1.5 Authorization

Authorization is the verification that the user is permitted to access any piece of information, which, in the context of this document, is the radio software for download. It is very important to verify that the entity trying to download radio software has the authority to receive, install and utilize it.

Radio software that is downloaded may be proprietary to the vendor or operator that developed it and thus need to be protected from unauthorized access. Unauthorized access to radio software could lead to fraud, disruption of service or denial of service attacks, which need to be prevented. In this regard, Appendix A-1 describes a number of threat scenarios that could arise from authorized access and presents a security threat model developed by the SDR Forum.

These considerations thus give rise to the following requirement:

Requirement: The download process shall employ an effective authorization procedure to verify that the entity requesting the radio software download has the authority to receive, install, and utilize the radio software download.

4.1.6 Capability Exchange

Different types of SDR devices support different software entities and parameter sets depending on their capabilities. When the network receives a radio software download request for an SDR device, it must first request a report on the capabilities of the SDR device. This capability exchange is necessary for the network to push the correct software entities and parameter sets to the SDR device requesting the download. It is needed to ensure that the SDR device can accept, install, and successfully run the downloaded software.

There are two steps in the capability exchange. The first step is a Capability Request message from the network to the SDR device. The second step is a Capability Response from the SDR device to the network. The Capability Response may include:

- Current SDR device configuration
- Type approval data
- API revisions supported
- Resident hardware resources
- Resident software profile
- Resident compilers and operating systems
- Resident licenses
- Memory capability
- Processing power
- Display capability
- User interface information

Based on the Capability Response, the network will select appropriate software entities and parameter sets to match SDR device capabilities. The selected software entities and parameter sets will be the ones downloaded to the SDR device. If the network server finds no matching software entities and parameter sets, the download process shall be terminated with a failure message back to the SDR device.

In addition, the network shall be responsible for providing information regarding its own capabilities to the SDR device. This information will let the SDR device know which modes of operation and services are available in the network. The network capability may be provided to the SDR device either through broadcast messages or individual messages as part of the Capability Exchange process.

Requirement: A capability exchange shall take place between the network and the SDR device prior to radio software download to enable the network to select appropriate software entities and parameters sets for the SDR device. If the network server finds no matching software entities and parameter sets, the download process shall be terminated with a failure message back to the SDR device. The network shall also inform the SDR device of its own capabilities, including supported modes of operation and available services.

4.1.7 Download Acceptance Exchange

Before the actual radio software download takes place, a Download Acceptance Exchange shall take place between the download server and the SDR device to set up the stage for the radio software download to take place. In the Download Acceptance Exchange, the download server provides information on type approval of the code, download procedures and schedules, installation procedures, billing and licensing options, and procedures to the SDR device in the form of a Download Installation Profile. The Download Installation Profile may include:

- Whether download is mandatory or optional;
- Download procedure (incremental or complete);
- Download schedule; installation options;

♦ Licensing and billing information and options.

Upon receiving the Download Installation Profile, the SDR device or the SDR device user (upon prompting) may select installation options and accept or reject the terms of the radio software download. As a final step in the Download Acceptance Exchange, the download server validates the options selected by the SDR device or SDR device user. If the selected options cannot be validated properly, or if the SDR device or user rejects the terms of radio software download, the download process shall be terminated with a notification back to the network or the SDR device as appropriate.

Requirement: Prior to the actual radio software download, there shall be a Download Acceptance Exchange between the download server and the SDR device to prepare for the radio software download.

4.1.8 Protection

Radio software download may involve the downloading of radio software with configuration parameters and data proprietary to the original equipment vendor, third party software vendor, or service provider. It is important to ensure that when this proprietary intellectual property is being downloaded to the SDR device, it is adequately protected from unauthorized access.

One method of protecting proprietary radio software while it is being downloaded is encryption. A common method of encryption is the public key encryption system that is widely used in the computer communications industry.

These considerations lead to the following requirement:

Requirement: The download process shall employ means, such as encryption, of protecting proprietary radio software and data during download to prevent unauthorized parties from gaining access to or altering this proprietary data or software.

4.1.9 Software Download

Once all the previous procedures have been cleared successfully, the software shall be downloaded from the download server to a buffer area within the SDR device according to the agreed download schedule.

Depending upon the medium through which the software is downloaded (e.g. wireline connection through TCP/IP, wireless connection via GPRS, UMTS, CDMA2000, etc.) there may be limited or extensive error correction and retransmission mechanisms to ensure the integrity of the downloaded software. After the download is complete, there shall be a final integrity test performed on the downloaded software. For example, cryptographic encapsulation or a cyclic redundancy test may be performed to check the integrity of the software. In case of an integrity test failure, the SDR device may request the download server to retransmit the software partially or fully.

The integrity of downloaded software can be cryptanalytically ensured using digital signatures. Public Key Technology (PKI) provides a private/public key pair. Each user has a private key that no one else has access to. Using the private key of the sender, the download can be encrypted. Then the public key of the sender can be used to decrypt the download. This provides authentication of the sender and integrity of this data but not confidentiality of the download. However, confidentiality can also be provided by a variation of the above procedure.

The downloaded radio software shall also be tested for authenticity to verify that the received piece of software is indeed what it was intended to be and that it has not been tampered with.

Upon successfully receiving the radio software download, the SDR device shall transmit an Acknowledge Safe Receipt message to the download server. The download server shall terminate the radio software download procedure when it receives the Acknowledge Safe Receipt message from the SDR device. Upon successfully receiving the radio software download, the SDR device shall also release the network connections/resources that were utilized for the download.

If for some reason the radio software download fails or is interrupted before completion, the download server must have the ability to mark the exact point of interruption and complete the download at a later time instead of starting over from the beginning.

Requirement: The software shall be downloaded to a buffer area in the SDR device and verified for integrity and authenticity. Upon successfully receiving the radio software download, the SDR device shall transmit an Acknowledge Safe Receipt message to the download server, which shall then terminate the download procedure. Upon successfully receiving the software download, the SDR device shall also release the network connections/resources that were utilized for the download. If for some reason the radio software download fails or is interrupted before completion, the download server shall have the ability to mark the exact point of interruption and complete the download at a later time instead of starting over from the beginning.

4.1.10 Installation

Once the radio software has been successfully downloaded to the SDR device, it can be installed. The installation process may be initiated either by the download server or the SDR device. At this stage, the downloaded software resides locally in a buffer that is accessible by the SDR device. Note, however, that there may have been a delay between the download of radio software and its installation, and that further changes to the radio software or hardware configuration of the SDR device could have occurred during this time. Due to this possibility, there may have to be an Internal Capability Exchange within the SDR device at the time of installation to determine whether the configuration of the SDR device remains acceptable for correct operation of the downloaded software. If it is determined during this Internal Capability Exchange that there is a capability mismatch then the installation process shall be terminated.

After the Internal Capability Exchange has been completed successfully, the SDR device may request an installation key from the download server. Prior to transmitting the installation key to the SDR device, the download server may initiate a billing and licensing negotiation with the SDR device. If the SDR device or user accepts the billing and licensing agreement, the download server may transmit the installation key. In case the SDR device refuses to accept the billing/licensing agreement, the download server shall deny an installation key, thus resulting in the termination of the installation process

Upon successful receipt of the installation key, the SDR device can install the downloaded radio software. Whether or not older versions of the radio software are saved or deleted is at the discretion of the manufacturer.

Requirement: The SDR device shall follow a process for installing the downloaded radio software that includes:

- An internal capability exchange within the SDR device to determine whether the configuration of the SDR device remains acceptable for correct operation of the downloaded radio software. If a mismatch occurs, the installation process shall be terminated with feedback to an appropriate network entity.
- The request of an installation key from the download server to grant permission to install the download radio software on the SDR device.
- Initiation of any necessary in-situ testing activities.

4.1.11 In-situ Testing

This is a provision for testing the downloaded software on the SDR device platform. Test vectors downloaded with the software are used within the test to verify whether the installed software and the reconfigured SDR device are operating as expected. It is anticipated that in-situ testing will be the responsibility of the device manufacturer.

Requirement: After installation of the downloaded software, in-situ testing shall be performed to validate the operation of the installed software and the reconfigured SDR device.

4.1.12 Non-repudiation Exchange

Upon successful installation and testing of the downloaded software, the SDR device shall transmit a Successful Installation message to the download server, permitting any final activation and billing to take place. This non-repudiation exchange is a positive verification of the SDR device user’s participation on the transaction.

Requirement: After successful installation and testing of the downloaded software, a non-repudiation exchange shall occur between the SDR device and the download server to confirm the successful installation of software and to permit any final activation and billing.

4.1.13 Reset and Recovery Procedures

Despite the existence of appropriate security measures and integrity tests, some SDR devices could become corrupted by downloaded software viruses or could malfunction due to unexpected interactions between pre-installed and downloaded radio software. Such SDR devices could transmit undesired RF signals that may disrupt the network or affect the performance of other users. Such SDR devices are classified as rogue devices [2].

The first requirement in controlling rogue SDR devices is a software architecture feature called Secure Software Box or Core Module, as shown in Figure 2. The software architecture of each reconfigurable SDR device must contain a Core Module consisting of software that is responsible for certain critical functions. These critical functions allow basic connectivity and monitoring, take corrective actions in case of major software malfunctions, and control the power of the SDR device. This Core Module software is not subject to reconfiguration and must not be altered by any software downloads. A best practices recommendation is that the Core Module should be sealed with encryption.

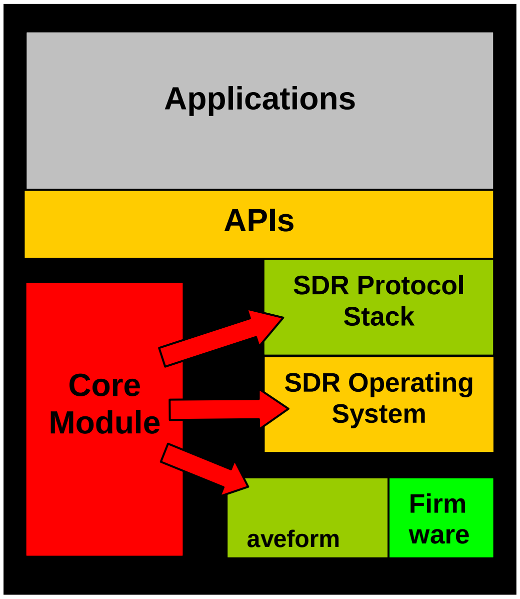


Figure 2: Software Architecture with Core Module for Reset and Recovery (adapted from [2])

An example reset and recovery system developed by the European Union (EU)-sponsored Transparently Reconfigurable UbiquitouS Terminal (TRUST) research project [1] is described below. Even though the TRUST project work specifically addresses reset and recovery for SDR terminals, we shall describe the reset and recovery system in general terms to make it applicable to any type of rogue SDR device, including SDR base stations. In this method of reset and recovery, rogue device identification is done either by the network (network-centric) or by the SDR device itself (SDR device-centric).

In the network-centric method, the network keeps monitoring how the SDR device responds to power control commands. If the device does not respond to power control commands, an algorithm is initiated that may result in resumption of services, reconnection attempts, or in the worst cases, corrective action to reconfigure the device or suspension of the device from any traffic channels. The network-centric method is mainly applicable when the SDR device is a mobile terminal.

In the SDR device-centric method, the rogue device identification and control is a little more elaborate and involves having a power measurement module inside the Core Module to monitor RF emissions from the SDR device. If the power measurement module detects any unauthorized emissions, the Core Module takes corrective actions according to a certain algorithm. This method may require the SDR device to have an additional receive chain built into the hardware to enable continuous monitoring even while the device is in active service. The SDR device-centric method is applicable to all types of SDR devices including mobile terminals and fixed base station type of SDR devices.

The above-described Core Module or secure software area may be used in conjunction with the download process to shut down the SDR device remotely when it is misbehaving beyond a certain limit. For example, assume that, after downloading and installing new radio software, the SDR device malfunctions, stops responding to normal reset and recovery procedures, and starts emitting energy at frequencies in which it is not allowed to operate. Upon detecting such a rogue device, the network operator may push some parameters or software to it, thus triggering the software in the Core Module to shut down the SDR device so that it can do no harm. The Core Module, combined with the download process, gives the network operator a powerful tool to control rogue SDR devices that may otherwise be harmful to the network and to other users of the network.

Requirement: The SDR device shall support a software architecture and reset and recovery procedure that enables the SDR device to recover from malfunctions caused as a result of installation of downloaded radio software. As part of this software architecture there shall be a secure software area in the SDR device that contains critical functions for basic connectivity, monitoring, corrective actions, and control of the SDR device's output power. This secure software area shall not be subject to reconfiguration and shall not be altered by any software downloads. When it is determined that the SDR device is severely malfunctioning, the secure software area, combined with the download process, shall enable the network operator to shut down the SDR device remotely to prevent it from doing harm. The reset and recovery system shall also audit key events and anamolies.

4.1.14 Termination

Termination is the last step in the radio software download process after all the above-specified steps have been completed. This step basically deals with cleaning up after the download is complete. The procedures that may be undertaken in this last step are:

- All databases and device parameter or capability tables residing on the network side and on the SDR device shall be updated to reflect the new configuration of the SDR device.
- Older versions of software residing on the SDR device may be deleted to free memory space.

Requirement: The final termination step in the radio software download process shall perform cleanup types of tasks such as updating all databases and device parameter or capability tables residing on the network side and the SDR device to reflect the new configuration of the SDR device, and deleting older versions of software residing on the SDR device to free memory space.

4.2 Requirements Specific to the SDR Device

4.2.1 Memory Management

When a software module is downloaded to an SDR device, the new software needs to be saved in the memory space available on the SDR device so that functions such as testing, installation, reconfiguration, and reset and recovery can be performed on the SDR device. In addition, other functions such as mode monitoring, service discovery, mode negotiation, mode switching, and reconfiguration management also need memory space on the SDR device. As a result a sophisticated SDR device must have additional memory space beyond that required for its normal mode of operation to be able to support radio software download and reconfiguration related functions.

Requirement: The SDR device shall be equipped with sufficient additional memory space beyond what is required for its normal mode of operation to support the functions such as mode monitoring, service discovery, mode negotiation, mode switching, radio software download, in-situ testing, installation, reconfiguration, reset and recovery, and reconfiguration management.

4.2.2 Identification of Alternative Modes of Operation

One of the advantages of a reconfigurable SDR device is that it can be reprogrammed to use modes of operation (air interfaces) other than the ones it currently supports. In order to for the SDR device to do this dynamically or on-the-fly, it needs to be aware of its current configuration, and needs to be able to continually monitor the presence of other modes of operation or air interfaces in its geographic area. If the SDR device's currently-supported modes of operation become unavailable or inadequate for the SDR device user's communication needs, the SDR device may reconfigure itself to support the mode of operation that is available and able to meet the SDR device user's communication needs. Alternatively, if a reconfigurable SDR device is turned on in a geographic area away from its home network, or if the SDR device is brand new and unconfigured, the SDR device may sense the available modes of operation in its geographic area, match them with the user's communication needs, and configure itself to support the selected mode of operation.

The requirement that arises from the above needs is as follows:

Requirement: The SDR device shall perform mode monitoring and service discovery to seek alternative modes of operation and services that are available in its current geographic area. The user shall be able to override the selection.

4.2.3 Selection of the Best Mode of Operation

Based on information obtained from the monitoring and service discovery tasks, or otherwise, the SDR device shall determine and select the most appropriate mode of operation for the desired service. For example, assume that a certain geographic area supports a wide-area network (WAN) and an 802.11-based local-area network (LAN), and that the SDR device user wishes to perform a videoconference call through the SDR device. In such a case, the SDR device shall determine whether the WAN or the LAN is better able to support the bandwidth/latency requirements of the videoconferencing application and shall select the better mode of operation to perform the desired service.

The best mode of operation shall also be selected for downloading radio software.

Requirement: The SDR device shall determine and select the most appropriate mode of operation for the desired service, including radio software download, subject to override by the user.

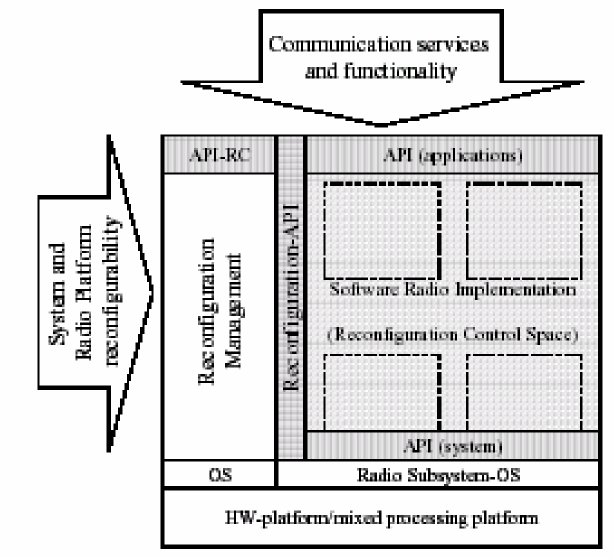
4.2.4 Reconfiguration Management

As the foregoing discussion makes clear, the radio software download process is complex and involves many different steps. It is envisioned[4] that there needs to be an overall management entity which oversees the radio software download process, especially the processes of radio software download, installation, reconfiguration, testing, and recovery. Such a Reconfiguration Manager (RM) is envisioned to consist of two parts, with one part residing in the SDR device (in the secure software area discussed in the previous section) and the other part residing on the network side (perhaps at the radio software download server). In this section we focus on the RM residing in the SDR device. The RM residing on the network side is discussed in section 4.3.4 as part of network requirements.

The RM residing in the SDR device shall oversee the entire radio software download process and be responsible for:

- Enabling full or partial reconfiguration of all protocol stack layers of the SDR device
- Controlling and managing reconfiguration processes at the SDR device
- Ensuring that any anticipated configuration adheres to the given radio access system standards and thus does not affect neighboring channels or systems, and
- Communicating with the RM residing on the network side to co-ordinate radio software downloads and reconfiguration

Figure 3 gives an example of an SDR device software architecture equipped with the above-described RM. The light-gray shaded area in the figure represents the reconfigurable radio software of the SDR device. This is the software that can be reconfigured to support enhanced or new air interface features, protocol layers, etc. There are various application program interfaces (APIs) to this reconfigurable software, one of which is the reconfiguration-API. The white area to the left of the reconfiguration-API represents the RM that is resident in the SDR device. The RM controls the reconfiguration of the radio software (light-gray area) in the SDR device through the reconfiguration-API.


Communication services and functionality
System and Radio Platform reconfigurability
API-RC
API (applications)
Reconfiguration Management
Reconfiguration-API
Software Radio Implementation
(Reconfiguration Control Space)
API (system)
OS
Radio Subsystem-OS
HW-platform/mixed processing platform

[4] Concepts presented in this sub-section are based on the research work described in reference [3].

Figure 3: SDR Architecture with Reconfiguration Management (reference [3])

For the purpose of radio software download the RM residing in the SDR device is the target of the downloaded software. For example, if the SDR device uses the MExE download protocol [4] for downloading radio software to the SDR device, the MExE entity residing in the SDR device would target the RM as the application for which the radio software is downloaded. The RM is envisioned to store the downloaded software in a local software repository before executing it to reconfigure the SDR device.

Note that the above discussion on RM does not preclude the SDR device from being an SDR base station.

Requirement: The SDR device shall be equipped with a Reconfiguration Manager (RM) that oversees the processes of radio software download, installation, reconfiguration, testing, and recovery. This RM shall reside in a secure software area in the SDR device that is not subject to reconfiguration. The RM shall be responsible for:

- Enabling full or partial reconfiguration of all protocol stack layers of the SDR device
- Controlling and managing reconfiguration processes at the SDR device
- Ensuring that any anticipated configuration adheres to the given radio access system standards and thus does not affect neighboring channels or systems
- Communicating with the RM residing on the network side to coordinate radio software downloads and reconfiguration

4.3 Requirements Specific to the Network Supporting the Download Process

4.3.1 Network Capacity and Spectrum Requirements

When the number of SDR devices downloading software in the network increases, the amount of network and spectrum resources used to support radio software download will also increase. The network operator must forecast and provision the radio network with enough network and spectrum resources to support radio software download traffic in addition to regular user traffic at a reasonable quality of service.

Requirement: The network operator shall forecast and provision the radio network with enough network and spectrum resources to support radio software download traffic in addition to regular user traffic at a reasonable quality of service.

4.3.2 Provision of Information Regarding Alternative Modes of Operation

One of the benefits of a network that supports radio software downloads and reconfigurable SDR devices is the ability of the SDR devices to reconfigure themselves to communicate in alternative modes of operation that may be available in a service area. For example, if a user with an SDR device roams to an area that supports a different air interface technology that is better suited for a specific service desired by the user, the SDR device may be reconfigured to support that air interface technology.

One fundamental requirement in the above scenario is that the SDR device is aware of which modes of operation (or air interface technologies) are available in a given area. Since this kind of information cannot be permanently stored on the SDR device, it becomes the network's responsibility to provide this information to the SDR device. The network may provide this information to the SDR device through one of several means, including broadcast control channel messages, common control channel messages, point-to-point information messages, etc. Moreover, this information about alternative modes of operation needs to be provided to SDR devices in the service area on a dynamic, real-time basis so that SDR devices get the most current status of the available modes of operation and can make informed decisions about mode switching.

Requirement: The network shall provide information to SDR devices regarding alternative modes of operation that are available in its service area. Moreover, the network shall provide this information about alternative modes of operation to SDR devices on a dynamic, real-time basis to allow SDR devices to make informed decisions about mode switching.

4.3.3 Roaming Support

In today's commercial cellular networks, network operators establish inter-carrier roaming agreements and appropriately populate subscriber databases to allow subscribers to roam on to each other's networks.

Radio software download may enable SDR devices to roam onto networks that support different air interface technologies because it enables the devices to download software and reconfigure themselves. For example, an SDR device that does not currently support the GSM cellular system could download radio software and reconfigure itself to support GSM when (or prior to) roaming to a network that supports GSM.

Roaming based on this type of dynamic SDR device reconfiguration is unprecedented. However, even in this case, the principles that support roaming remain exactly the same as in cellular networks today. Even with the advent of reconfigurable SDR devices, network operators still need to have inter-carrier agreements in place and still need to have subscriber databases appropriately populated in order to enable subscribers to roam on to other networks.

In other words, the existing principles of roaming apply exactly to dynamically reconfigurable SDR devices.

Requirement: Dynamically reconfigurable SDR devices shall be able to roam onto other networks using the same principles of roaming that are used in commercial cellular networks today.

4.3.4 Network Architecture Requirements

As the number of SDR devices deployed in the network increases, the network architecture needs to have certain features to be able to support radio software downloads efficiently. Moreover, as the number of SDR devices increases in the network, the network needs an overall management entity to track configurations of various SDR devices in the network and to coordinate the download and reconfiguration processes. Section 4.2 discussed the concept of a Reconfiguration Manager (RM) in the context of the SDR device. In this section we present the concepts and requirements of an RM entity residing on the network side.

In earlier sections of this document, we had used the term SDR server or download server for the network entity from which the SDR device downloads radio software. In this section we will expand this term to include a broad network RM entity, whose functionality may be distributed among multiple network elements. This broad RM entity shall be responsible for:

- Maintaining a database of current configurations and capabilities of SDR devices in the network
- Scheduling radio software downloads to SDR devices (in the case of mass SDR device upgrades for bug-fixes or version changes, the RM may schedule radio software downloads at times when there is low user traffic in the network)
- Providing a network architecture that is able to support efficient downloads to large number of SDR devices
- Maintaining software repositories of original equipment manufacturer (OEM) software modules, and coordinating SDR device access to these repositories for efficient downloads
- Communicating with local RMs residing on each SDR device to coordinate download and reconfiguration processes, and
- Communicating with local RMs residing on each SDR device to coordinate and assist with mode identification, mode monitoring, mode negotiation, and mode switching

As an illustration of a network architecture that satisfies the above requirements, consider the architecture shown in Figure 4. This architecture has been developed as part of the EU’s TRUST research project [5] and assumes that the SDR devices are mobile terminals. The architecture includes a Home Reconfiguration Manager (H-RM) that resides in the user’s home network. There is a corresponding Serving Reconfiguration Manager (S-RM) and Proxy Reconfiguration Manager (P-RM) in the Access Network. The H-RM and the S-RMs have access to a Software Repository that stores the sets of software that may be downloaded by the terminals. The H-RM maintains a Terminal Database that holds information about the capabilities and current configurations of terminals. In addition to this the H-RM also has access to several terminal manufacturers and software providers in order to receive the latest software upgrades. The entire architecture is designed so that it is able to handle upgrades even to a large number of terminals in the system.

This TRUST architecture envisions two types of deployment scenarios: terminal-centric and network-centric. In the network-centric deployment, the P-RM plays an important role by acting as a proxy for the SDR terminal in performing the majority of negotiations with the S-RM and H-RM on behalf of the terminal. The P-RM provides information for mode identification and monitoring, mode negotiation and switching, radio software download, and reconfiguration. By performing these roles on behalf of the SDR terminal, the P-RM reduces the load on the wireless link and decreases the CPU and battery load of the SDR terminal. Since the terminal does not have to perform these roles, it leads to a simpler terminal design. In the terminal-centric mode there is no need for a P-RM and all functionality is built into the SDR terminal. For more information on this TRUST research project, please see references [5] and [6].

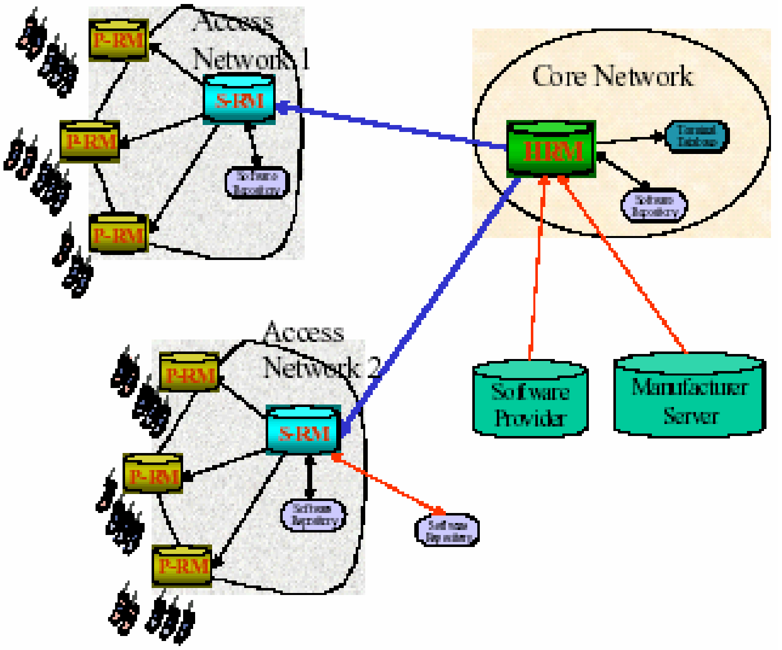


Figure 4: Example Network Architecture with Reconfiguration Management (Reference [5])

Requirement: The network architecture shall support the following reconfiguration management functionalities to control and coordinate radio software download and SDR device reconfiguration in the network:

- Maintaining a database of current configurations and capabilities of SDR devices in the network
- Scheduling radio software downloads to SDR devices
- Providing a network architecture that is able to support efficient downloads to large number of SDR devices

- Maintaining software repositories of third-party vendor and original equipment manufacturer (OEM) software modules, and coordinating SDR device access to these repositories for efficient downloads
- Communicating with local RMs residing on each SDR device to co-ordinate download and reconfiguration processes
- Communicating with local RMs residing on each SDR device to co-ordinate and assist with mode identification, mode monitoring, mode negotiation, and mode switching
- Standardized auditing

4.4 Security Considerations

Security requirements for commercial wireless need to be such that techniques to fulfill these requirements can be met at a reasonable cost while at the same time fulfilling the basic requirement that malicious code cannot be downloaded and activated.

Security measures can be divided generically into the following six general categories:

- *Trusted System Operation*: Confidence that software will execute in the device exactly as intended. SDR security will require some elements to be enforced by hardware measures. Such hardware measures are needed to ensure that there is a root security mechanism that cannot be modified by software changes. Trusted system methodology is however expensive and should probably only be used on high end SDR devices.
- *Authentication:* The ability to validate the origin of received information. For example, an SDR device should be able to ensure prior to installation that the downloaded software originates from a trusted server. The SDR device should install only authenticated software.
- *Authorization:* Verification that the user is permitted to access the data or to utilize a communications capability.
- *Integrity:* Verification that received information has not been modified or corrupted in transit. Prior to accepting and installing new software, an SDR device should be able to ascertain that, since originating from the trusted server, the downloaded data has not been modified. The SDR unit should only install software that has been checked for its integrity. It is critically important to bear in mind that because we are dealing with software defined radios, threats can be realized during the loading, installation and activation or instantiation of software. Integrity verification is needed during each of these phases.
- *Privacy:* Often referred to as "confidentiality," this category usually refers to the assurance that other parties cannot access a user's personal information. In the case of SDR, however, privacy can apply not only to user data, but also to the executable software, which is the intellectual property of the equipment manufacturer or software developer. Encryption techniques may be used to prevent unauthorized parties from gaining access to private user data, or to proprietary software.
- *Non-repudiation:* Positive verification of a sender or receiver's participation in a transaction.
- *Auditing:* Versions, upgrades, security events, etc. among other types of audits.

All of these general security requirements are also requirements for the more specific challenges of SDR security. Security requirements are directly related to the anticipated threats to the communication service or system. The SDR Forum has developed a threat model, and this model is described in Appendix A. In general, threats are the same for terminals as they are for base stations. Because of differences in regulatory policies around the globe, a security policy mechanism needs to be downloadable.

4.5 Protection Profiles

The SDR Forum is considering studying Protection Profiles as a requirement that will be included in future versions of this document. A Protection Profile is an implementation independent statement of security requirements that is shown to address threats that exist in a specified environment. Protection profiles are registered through national processes. Protection Profiles are now becoming a standard requirement for the Common Criteria – the international mechanism for certification and accreditation of security devices.

Further information on protection profiles may be found at the following URLs:

Protection profile information:
http://www.commoncriteria.org/protection_profiles/pp.html

Common Criteria URL:
http://niap.nist.gov/cc-scheme/PPRegistry.html

Some protection profiles:
http://www.radium.ncsc.mil/tpep/library/protection_profiles/

5 Summary

This section summarizes all the radio software download requirements defined in this document.

Functional Requirement		Summary of Requirement	Section
1	Discovery of the need for download	**Requirement**: The radio software download process shall allow discovery of the need for radio software download to be made by the application, the SDR device, the network, the network/service provider, or the user.	4.1.1
2	Download initiation	**Requirement**: The download process, SDR device, and network shall be capable of supporting download initiation by the application, the SDR device, the network, the network/service provider, or by human intervention (user or technician).	4.1.2
3	Download setup	**Requirement**: The download process shall have the equivalent of a Download Setup stage, which decides, based on the reason for download, which steps in the download process need to be executed, with what security provisions, and in which order.	4.1.3

Functional Requirement		Summary of Requirement	Section
4	Mutual authentication	**Requirement**: The download process shall employ a rigorous mutual authentication procedure for validating the identities of the SDR device (hardware and software), the user, the service provider, the network operator, the manufacturer, and the regulatory organization, prior to allowing the download of radio software to the SDR device.	4.1.4
5	Authorization	**Requirement**: The download process shall employ an effective authorization procedure to verify that the entity requesting the radio software download has the authority to receive, install, and utilize the radio software download.	4.1.5
6	Capability exchange	**Requirement**: A capability exchange shall take place between the network and the SDR device prior to radio software download to enable the network to select appropriate software entities and parameters sets for the SDR device. If the network server finds no matching software entities and parameter sets, the download process shall be terminated with a failure message back to the SDR device. The network shall also inform the SDR device of its own capabilities, including supported modes of operation and available services.	4.1.6
7	Download acceptance exchange	**Requirement**: Prior to the actual radio software download, there shall be a Download Acceptance Exchange between the download server and the SDR device to prepare for the radio software download.	4.1.7
8	Encryption	**Requirement**: The download process shall employ means, such as encryption, of protecting proprietary radio software and data during download to prevent unauthorized parties from gaining access to or altering this proprietary data or software.	4.1.8
9	Software download	**Requirement**: The software shall be downloaded to a buffer area in the SDR device and verified for integrity and authenticity. Upon successfully receiving the radio software download, the SDR device shall transmit an Acknowledge Safe Receipt message to the download server, which shall then terminate the download procedure. Upon successfully receiving the software download, the SDR device shall also release the network connections/resources that were utilized for the download. If for some reason the radio software download fails or is interrupted before completion, the download server shall have the ability to mark the exact point of interruption and complete the download at a later time instead of starting over from the beginning.	4.1.9
10	Installation	**Requirement**: The SDR device shall follow a process for installing the downloaded radio software that includes: ♦ An internal capability exchange within the SDR device to determine whether the configuration of the SDR device remains acceptable for correct operation of the downloaded radio software. If a mismatch occurs, the installation process shall be terminated with feedback to an appropriate network entity. ♦ The request of an installation key from the download server to grant permission to install the download radio software on the SDR device. ♦ Initiation of any necessary in-situ testing activities.	4.1.10
11	In-situ testing	**Requirement**: After installation of the downloaded software, in-situ testing shall be performed to validate the operation of the installed software and the reconfigured SDR device.	4.1.11

Functional Requirement		Summary of Requirement	Section
12	Non-repudiation exchange	**Requirement**: After successful installation and testing of the downloaded software, a non-repudiation exchange shall occur between the SDR device and the download server to confirm the successful installation of software and to permit any final activation and billing.	4.1.12
13	Reset and recovery	**Requirement**: The SDR device shall support a software architecture and reset and recovery procedure that enables the SDR device to recover from malfunctions caused as a result of installation of downloaded radio software. As part of this software architecture there shall be a secure software area in the SDR device that contains critical functions for basic connectivity, monitoring, corrective actions, and control of the SDR device's output power. This secure software area shall not be subject to reconfiguration and shall not be altered by any software downloads. When it is determined that the SDR device is severely malfunctioning, the secure software area, combined with the download process, shall enable the network operator to shut down the SDR device remotely to prevent it from doing harm. The reset and recovery system shall also audit key events and anamolies.	4.1.13
14	Termination	**Requirement**: The final termination step in the radio software download process shall perform cleanup types of tasks such as updating all databases and device parameter or capability tables residing on the network side and the SDR device to reflect the new configuration of the SDR device, and deleting older versions of software residing on the SDR device to free memory space.	4.1.14
15	Memory management	**Requirement**: The SDR device shall be equipped with sufficient additional memory space beyond what is required for its normal mode of operation to support the functions such as mode monitoring, service discovery, mode negotiation, mode switching, radio software download, in-situ testing, installation, reconfiguration, reset and recovery, and reconfiguration management.	4.2.1
16	Identification of alternative modes of operation	**Requirement**: The SDR device shall perform mode monitoring and service discovery to seek alternative modes of operation and services that are available in its current geographic area. The user shall be able to override the selection.	4.2.2
17	Selection of best mode of operation	**Requirement**: The SDR device shall determine and select the most appropriate mode of operation for the desired service, including radio software download, subject to override by the user.	4.2.3
18	Reconfiguration management	**Requirement**: The SDR device shall be equipped with a Reconfiguration Manager (RM) that oversees the processes of radio software download, installation, reconfiguration, testing, and recovery. This RM shall reside in a secure software area in the SDR device that is not subject to reconfiguration. The RM shall be responsible for: ♦ Enabling full or partial reconfiguration of all protocol stack layers of the SDR device ♦ Controlling and managing reconfiguration processes at the SDR device ♦ Ensuring that any anticipated configuration adheres to the given radio access system standards and thus does not affect neighboring channels or systems ♦ Communicating with the RM residing on the network side to coordinate radio software downloads and reconfiguration	4.2.4

Functional Requirement		Summary of Requirement	Section
19	Network capacity and spectrum requirements	**Requirement**: The network operator shall forecast and provision the radio network with enough network and spectrum resources to support radio software download traffic in addition to regular user traffic at a reasonable quality of service.	4.3.1
20	Provision of information regarding alternative modes of operation	**Requirement**: The network shall provide information to SDR devices regarding alternative modes of operation that are available in its service area. Moreover, the network shall provide this information about alternative modes of operation to SDR devices on a dynamic, real-time basis to allow SDR devices to make informed decisions about mode switching.	4.3.2
21	Roaming support	**Requirement**: Dynamically reconfigurable SDR devices shall be able to roam on to other networks using the same principles of roaming that are used in commercial cellular networks today.	4.3.3
22	Network architecture requirements	**Requirement**: The network architecture shall support the following reconfiguration management functionalities to control and coordinate radio software download and SDR device reconfiguration in the network: ♦ Maintaining a database of current configurations and capabilities of SDR devices in the network ♦ Scheduling radio software downloads to SDR devices ♦ Providing a network architecture that is able to support efficient downloads to large number of SDR devices ♦ Maintaining software repositories of third-party vendor and original equipment manufacturer (OEM) software modules, and coordinating SDR device access to these repositories for efficient downloads ♦ Communicating with local RMs residing on each SDR device to co-ordinate download and reconfiguration processes ♦ Communicating with local RMs residing on each SDR device to co-ordinate and assist with mode identification, mode monitoring, mode negotiation, and mode switching ♦ Standardized auditing	4.3.4

6 References

[1] "Overview and Definition of Software Download for RF Reconfiguration," SDR Forum Document Number SDRF-02-T-0001-V2.10, June 2002.

[2] http://www.ist-trust.org

[3] J. Faroughi-Esfahani, N. Greco, G. Vardoulias, and N. Drew, "Detection and Control of the Rogue SDR-terminals in the Future Network," SDR Forum Document Number SDRF-01-I-0048-V0.00, Aug 2001.

[4] K. Moessner and R. Tafazolli, "Software Radio Integration and Reconfiguration Management," SDR Forum Document Number SDRF-01-I-0064w-V0.00, Oct 2001.

[5] "Mobile Execution Environment (MExE); Functional Description; Stage 2," Third Generation Partnership Project, Technical Specification 3GPP TS 23.057.

[6] N. Olaziregi and D. Bourse, “Architectures Supporting SDR Terminals,” SDR Forum Document Number SDRF-01-I-0050w-V0.00, Aug 2001.

[7] J. Hoffmeyer, S. Blust, R. Moton, M. Chartier, “Information Document: ITU-R Work in Software Defined Radio,” SDR Forum Document, Jan 2002.

[8] “Security Threats and Requirements Technical Specification, Group Services and Systems Aspects,” Third Generation Partnership Project, 3GPP TS 21.133 V4.1.0 (2001-12); available at ftp://ftp.3gpp.org/specs/archive/21_series/21.133/21133-410.zip

[9] K. Riordan, “SDR Security Threats and Requirements,” Motorola, Inc., June 2002.

Appendix A: Security Threat Scenarios and SDR Security Threat Model

For SDR-capable devices, security threats can be described using a four-part model, as illustrated in Figure A-1. This model builds on the model described in reference [9] by incorporating the “point of attack” categorization of 3GPP as described in reference [7]. The model is responsive to the fact that requests for updates may come from the terminal to the network as well as the requirement that updates may be originated by the network; where the updates originate has an impact on how one should categorize or model the SDR threat scenarios.

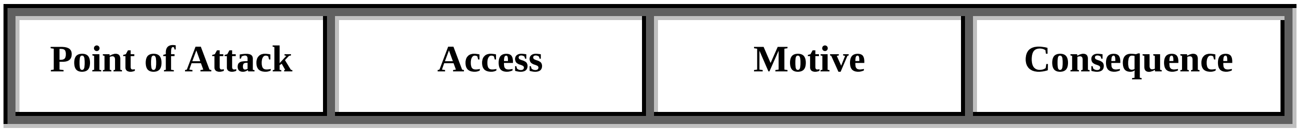


Figure A-1: Four-part SDR Security Threat Model

Point of Attack[5]: This refers to the device or system component within the communication system where the security breach occurs. (Note: the point of attack is not necessarily the same as the target of the attack. For example, the target could be the population of terminals operating within a wireless network, whereas the point of the attack could be the network that provides services to those terminals.) The following points of attack are considered in this model:

- **Terminals and UICC/USIM:** The security breach occurs at the handset or other terminal equipment. Access to the terminal may be physical or remote as defined by the “Access” parameter.
- **Infrastructure**: The security breach occurs within the Radio Access Network or Core Network. Access to the Infrastructure may be physical or remote as defined by the “Access” parameter.

[5] The point of attack categorization is based on the 3GPP categorization of the point of attack for threats against 3G wireless systems [Reference 7]. The threat against SDR-capable devices is expected to be a subset of the general wireless threat identified by 3GPP. The SDR threat model is still under study by the SDR Forum. The SDR Forum has the view that the general security threat against wireless systems is well understood and that the SDR-capable base stations and terminals may not require any additional security measures in the network infrastructure. Nevertheless, a full understanding of the security threats to SDR-capable devices requires an understanding of the security measures in place in the network infrastructure. Therefore, it is important to include the “point of attack” component in this model.

Access: This refers to the means by which the perpetrator obtains access to the Point of Attack.

- **Physical**: The threat requires physical control of, or access to, the device or network entity.
- **Remote**: The threat can be perpetrated remotely, by exploiting some external interface to the device or network entity, including wireless interfaces.

Motive: Motive refers to the motivation of the party responsible for the threatening action.

- **Negligent**: Accidentally harmful consequences of a legitimate action. (e.g. the download of authenticated software which contains an unintentional software "bug")
- **Unauthorized**: Unintentionally harmful consequence of an improper or unauthorized action. (e.g. download of unauthorized black market software which is advertised to "boost" handset performance)
- **Malicious**: Deliberate, improper action, specifically intended to cause harmful consequences.

Consequence: This refers to the nature of the harmful consequence resulting from the threatening action.

- **Denial of Service (DoS)**: Widespread impairment of the Quality of Service (QoS) for users of the network, on which, the attack was perpetrated.
- **Interference with other Services**: widespread performance impairment of, or improper access to, other networks or services.
- **Digital Rights Violation**: Unauthorized access to, or theft of, digital content and software.

The point of attack, access means, motivation, and consequence are variables in the description of a security threat. There are, therefore, **2 x 2 x 3 x 3 = 36** unique categories of threats. For each of these categories, there are many variations and permutations, resulting in a boundless array of unique threat scenarios. It is, however, sufficient to focus on the simple four-part security threat model when considering the necessary security counter-measures (as discussed in later sections).

The SDR Forum holds the view that the issues, problems, and solutions associated with security aspects of SDR must be addressed from a "systems" perspective. The four-part model described above supports this viewpoint. As an example to illustrate this systems perspective (and supported by figures A-2 and A-3), we consider here the authorization and download of radio software and the mechanisms needed to insert the radio software into a terminal (handset). The SDR software download example is illustrated in Figure A-2.

The data source for the software download may originate either internal or external to the wireless system, as illustrated in Figure A-2. The information flow may go out over the radio interface and thus come through the core network. It is entirely possible for the data and information to be downloaded to originate outside the radio system and the core network (e.g., from a manufacturer's system) where presumably the network operator and the service provider (who may or may not be the same entity or company) have "reviewed and authorized" the download of the radio software. In this case, the security, integrity and threats are many and can occur at numerous points in the entire process.

Thus, at the onset it is a systems view that must be taken. As we move forward into the details of the system and subsystems, then more and more specific models and analysis are required to address the details of the issues.

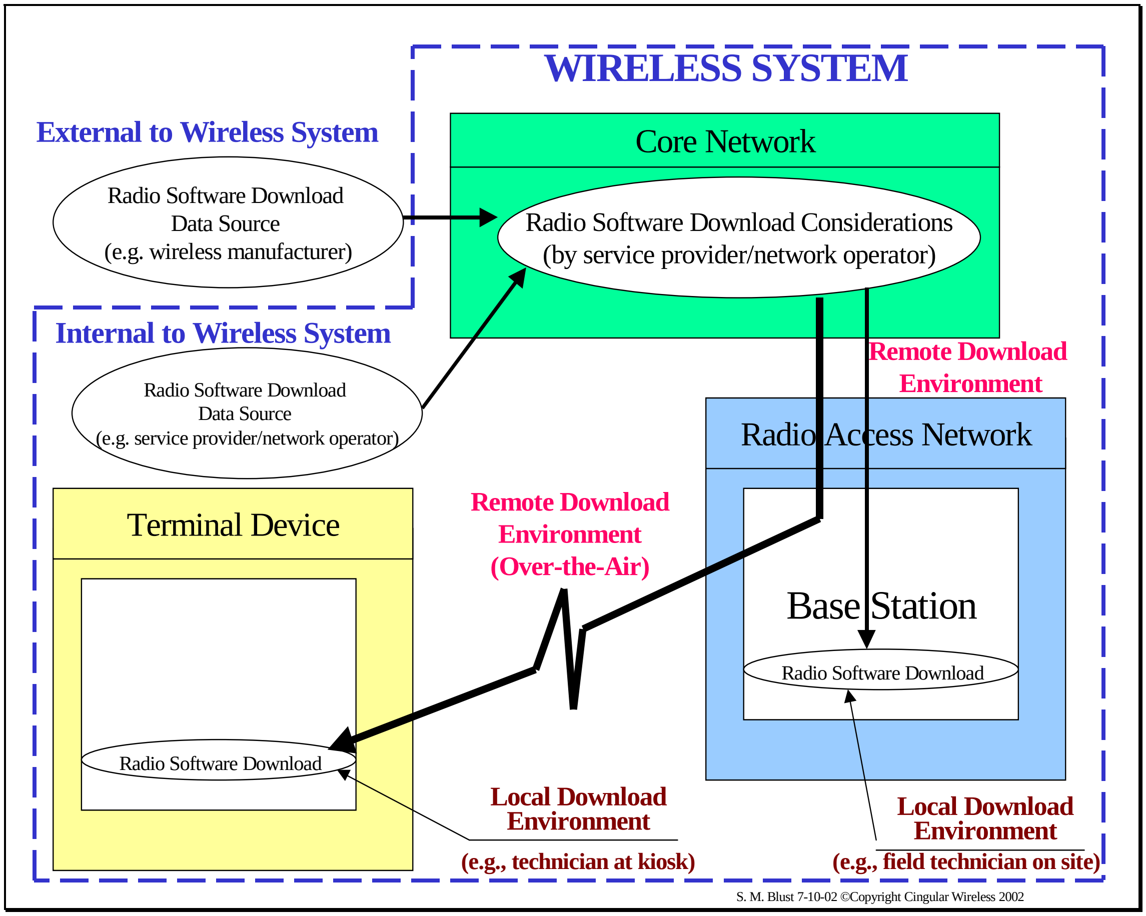

WIRELESS SYSTEM
External to Wireless System
Radio Software Download Data Source (e.g. wireless manufacturer)
Core Network
Radio Software Download Considerations (by service provider/network operator)
Internal to Wireless System
Radio Software Download Data Source (e.g. service provider/network operator)
Remote Download Environment
Radio Access Network
Base Station
Radio Software Download
Terminal Device
Remote Download Environment (Over-the-Air)
Radio Software Download
Local Download Environment
(e.g., technician at kiosk)
Local Download Environment
(e.g., field technician on site)
S. M. Blust 7-10-02 ©Copyright Cingular Wireless 2002

Figure A-2: Radio Software Download System Flow Example

Figure A-3 depicts the characterization of software download. In this report, we are only concerned with the download of radio software (that is, software for RF reconfiguration) as opposed to the download of non-radio software. In other words, the ellipses in the terminal device and radio access network in Figure A-2 is the software encircled with the loop in Figure A-3. Furthermore the following definitions are used for the primary radio software (which is of particular interest to regulators) and the ancillary radio software:

> *Primary radio software:* Software that affects the radio functionality (e.g., frequency, power, and modulation). The primary software within a wireless device is tightly coupled with the radio hardware to derive the overall radio functionality.
>
> *Ancillary radio software*: Software that affects the use of the device, but does not affect the radio functionality. Input/output drivers and user interfaces are examples of ancillary radio software download.

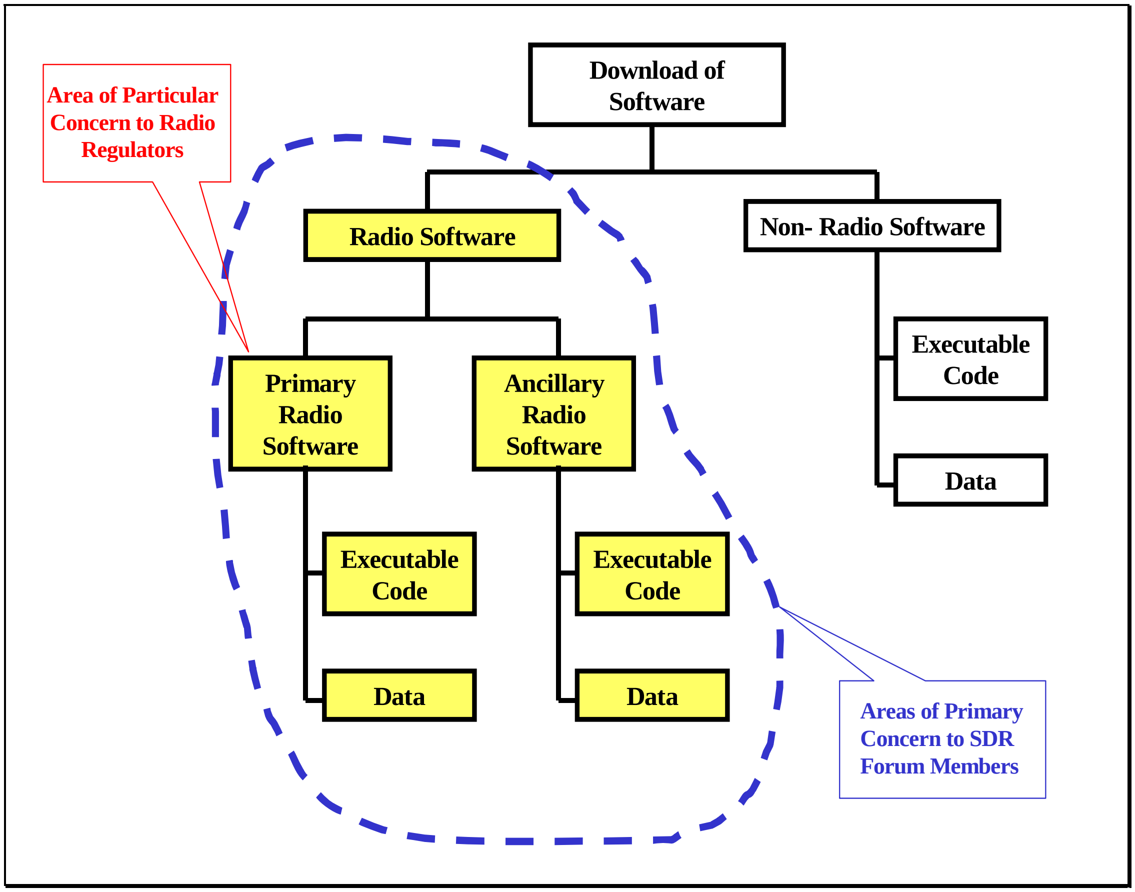


Figure A-3: Characterizations of Software Download

Table A-1 contains several example security threats, and also illustrates how the four-part model can be used to classify a given threat.

Table A-1: Examples of SDR Security Threat Scenarios

Example Threat Scenario		Point of Attack	Access	Motive	Consequence
1	A sophisticated hacker creates and distributes a virus or malicious application that causes widespread interference **to other communication systems**, such as public safety, emergency, and navigation control communication systems.	Terminal	Remote	Malicious	Interference
2	A sophisticated hacker creates and distributes a virus or malicious application that corrupts the operation of SDR terminals in a manner, which causes widespread disruption of service **to the affected communication system**.	Terminal	Remote	Malicious	Denial of Service
3	Manipulation of signalling or control data: Intruders may modify, insert, replay, or delete signalling or control data on any stem interface.	Infrastructure	Remote	Malicious	Denial of Service
4	A black market company creates and distributes a rogue application which causes an SDR terminal to deviate from its normal performance limits, and in so doing, causes widespread disruption of service to the affected communication system. (As an example, consider an application that causes the terminal transmitter to always transmit at maximum power, ostensibly allowing the user to get better performance, yet actually degrading the overall performance of the system).	Terminal	Remote	Unauthorized	Denial of Service
5	An unethical company takes in old model phones, illegally reprograms and resells the devices as "new" on the black market. The hardware/software combination of the modified phones is unreliable, and causes the devices to eventually "crash" (i.e. suffer an unrecoverable failure)	Terminal	Physical	Unauthorized	Denial of Service
6	A new release of software inadvertently contains a "bug" and is distributed to users in the network. The bug causes terminals to reset unexpectedly, causing widespread denial of service.	Terminal	Remote	Negligent	Denial of Service

(Table A-1, continued)

Example Threat Scenario		Point of Attack	Access	Motive	Consequence
7	An unethical company intercepts software downloaded to phones operating in the network, and illegally re-uses the software to build and sell black market devices.	Terminal	Remote	Malicious	Digital rights
8	An unethical company modifies the electronic identifier information on phones intended for sale in one country, and profitably resells the phones in another country where the sale is not legal. (As an example: low cost phones with reduced spectral emission specifications may be legal in one country, but illegal in another country).	Terminal	Physical	Unauthorized	Interference
9	Disreputable parties modify device software, causing them to transmit and/or receive on different frequencies, thus enabling covert communications or eavesdropping.	Terminal	Physical	Malicious	Interference

A wireless base station or handset, employing SDR technologies, should be protected against the threats described above. Achieving robust security must be accomplished through a combination of inherent limitations in the programmability of the unit (as discussed in Section 8 of reference [9]), and the addition of specific security features (such as those discussed in Section 9 of reference [9]).