SOFTWARE DEFINED RADIO SOLUTIONS
A MILITARY RADIO PERSPECTIVE

Mark R. Turner (Harris Corporation, Rochester New York; e-mail: mark.turner@harris.com)

ABSTRACT

Military Radio development in the United States is being driven by the key U.S. Department of Defense (DoD) transformational program, the Joint Tactical Radio System (JTRS). The foundation of the JTRS Program is built on Software Defined Radio (SDR) solutions and associated technology in order to meet today's and tomorrow's war-fighters' radio communications needs. This paper summarizes these military SDR requirements for JTRS, provides a brief description of the Harris Falcon II family of military SDRs and how Harris has leveraged this experience and technology into the JTRS Program as a model for scalable SDR solutions. A detailed description of Information Security solutions for JTRS is provided, and a description of the Harris JTRS Step 2B Program including technical results and observations. A discussion of software efficiency optimization techniques for battery powered platforms is also provided.

1. INTRODUCTION

Harris Corporation is a multi-level participant in the overall JTRS Program, with three currently active JTRS contracts, including: the Step 2B Program, the Cluster 1 Program and the Cryptographic Equipment Application (CEA) Program. The JTRS Step 2B Program includes validation of the Software Communications Architecture (SCA) for battery-powered, Man-pack radio (MPR) and Hand-held (HH) radio platforms requirements, using Harris Sierra™ security technology. Harris Corporation is an integral member of the winning JTRS Cluster 1 Boeing team, developing waveforms for the JTRS waveform library, developing the security architecture for the overall radio system, developing several key hardware Line Replaceable Units (LRUs) for the Cluster 1 JTR Set and also developing the Cryptographic Subsystem (CSS) using Harris Sierra™ security technology. The JTRS CEA Program involves the development of software applications, implementing the required modes of specific cryptographic equipment.

2. JOINT TACTICAL RADIO SYSTEM

" DoD Vision for SDR Solutions"

The objective of the Joint Tactical Radio System Program is to define and acquire a family of multi-mode, multi-band, programmable SDRs to increase operational flexibility, enhance Joint and Coalition interoperability, and reduce life cycle cost. These radio systems will provide network-centric capabilities and enable mission flexibility for the DoD Joint Vision 2020.

As stated in the JTRS Operational Requirements Document (ORD), JTRS is required to provide interoperability across all geographical and organizational boundaries – horizontal and vertical, so as to create an interoperable information transfer capability for Joint and Coalition operations. JTRS will be capable of transmitting voice, data, and video while operating in frequency bands from 2 MHz to 2 GHz, with the potential to increase the top end frequency to 55 GHz to satisfy space communications requirements. By placing a premium on joint and coalition interoperability, the JTRS program focuses on solving interoperability issues currently with Services' legacy radios.

To facilitate the building of the JTRS family of radios, the JTRS Joint Program Office (JPO) tasked industry to develop and validate the SCA. The SCA consists of a set of rules and protocols, which define a Common Open Standards Architecture for SDR applications, making maximum use of commercial standards and APIs. This architecture supports implementation of SDR waveform applications and JTRS Set hardware that can be re-used across multiple operational environments. In addition, the SCA is intended to facilitate technology insertion into JTR Sets over the life cycle of the radio and to leverage advances in commercial radio markets (such as cognitive radio).

The SCA utilizes Component Based Development (CBD) technology which has the potential to become the "industrial revolution" of software, promoting the advent of interchangeable software parts, built to predefined specifications. With respect to SDR solutions, the ability to reuse existing software components across multiple radio applications in an open framework, and the encapsulation of hardware specific capabilities and platform services through well-defined Application Programmer Interfaces (APIs) will facilitate true waveform portability both from practical application and affordability perspectives.

3. HARRIS MILITARY RADIO SOLUTIONS

"Meeting the War-fighter's Needs"

Harris developed the Falcon II radio family as a third generation set of SDRs, with the true integration of radio and computer and technologies. Harris has fielded over 20,000 of these radios including: HH radios, Man-pack Radios and ground vehicular radio applications. The Falcon II radio family provides full software re-programmability, hardware re-programmability, run-time hardware re-configuration and large object-oriented software implementations (3 million source lines of code). These radios cover the spectrum from 2 MHz to 512 MHz, providing high performance Line-of-Sight (LOS) and Beyond-Line-of-Sight (BLOS) communications (High Frequency and UHF Tactical Satellite Communications). Falcon II radios are fully secure, including Type I and exportable, customizable cryptography (see figure 3.0-1).

Figure 3.0.1
Harris Falcon II
Radio Family

Harris has leveraged this unprecedented experience to develop JTRS radio solutions that truly meet the war-fighter's needs. Harris has demonstrated multi-channel, fully secure portable radio configurations that provide JTRS compliant LOS and BLOS communications, but more importantly meet the performance expectations of the war-fighter.

4. INFORMATION SECURITY SOLUTIONS

"Securing the Mission and protecting the User"

Information Security (INFOSEC) is a key component to the success of the JTRS Program, including the development and deployment of a programmable INFOSEC module. Without a programmable INFOSEC module the flexibility and growth capability of a JTRS-compliant system will be limited by legacy cryptographic equipment or require expensive hardware upgrades. The rapid evolution of the Internet and advent of wireless networking is dictating the development of next-generation cryptography. The development and integration of programmable cryptographic module will allow JTRS-compliant systems to download new cryptographic algorithms and functions in conjunction with new or updated waveform capabilities.

The Harris Sierra™ family of security devices provides advanced INFOSEC solutions across all JTRS radio domains and for other applications. Harris Sierra™ devices are small in size (refer to figure 4.0-1) and are designed with a scalable, building block architecture based on the latest System-on-a-Chip (SoC) technology. This scalable architecture facilitates the combination of cryptographic functions and key management functions into a single chip or allocation of these functions across multiple chips for solutions which require multiple levels of security (Multiple Single Levels of Security - MSLS). The Sierra™ cryptographic functions include a broad set of capabilities, including: encryption/decryption, transmission security, authentication and integrity, certificate and policy management.

Figure 4.0-1 Harris
Sierra Module

Sierra™ devices provide an optimal combination of hardware and software components to maximize performance: including throughput and power utilization. The Sierra™ II device fully supports the demanding throughput performance of the JTRS Wideband Networking Waveform (WNW). Sierra™ devices employ chip level power management, automatically disabling unused internal circuitry dependent on security channel configuration to minimize power consumption (not possible with software only security device implementations). The unique scalability of the Harris Sierra™ architecture, make it the only INFOSEC solution to meet the broad requirements across the diverse set of JTRS domains (from Small Form-Factor platforms, to man-portable radio platforms, ground vehicular platforms to large full-scale communications systems for shipboard platforms and fixed sites).

Cryptographic Equipment Applications (CEA) are Software Product Configuration Items (SPCI) that

implements one or more operational modes of cryptographic equipment. CEAs are specific to a particular cryptographic hardware device. Harris is under contract with the JTRS JPO to develop Sierra™ CEAs for the JTRS JPO Library. Harris Sierra™ software utilizes a modular, building block architecture, which facilitates the porting of CEAs across all JTRS radio domains and specific hardware platforms with minimal porting cost and time (refer to figure 4.0-2).

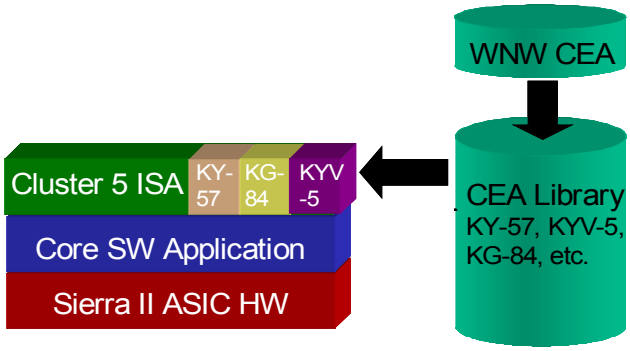

Figure 4.0-2 Sierra™ Software Architecture

The lowest layer of the Sierra™ II software architecture consists of the essential software burned into the ASIC hardware. The next layer is the Core Software Application which provides a set of essential services for CEAs, such as file services and key management. These first two layers of the Sierra™ II software architecture are certified by the NSA, in conjunction with the Sierra™ II ASIC hardware as basis for each individual host embedment to build upon. The Independent Software Application (ISA) layer supports platform specific hardware/software interfaces, which are unique for each host embedment. The CEAs required to support a waveform application and other radio platform functions are extracted from the JTRS JPO CEA Library and integrated with the platform specific ISA. The integrated ISA/CEA executable image is signed by NSA following the certification process and upon installation, is stored within a Sierra™ II based Cryptographic Subsystem (CSS) following signature authentication.

5. HARRIS JTRS STEP 2B PROGRAM

"Bringing it all together in <u>real</u> JTRS radios"

The objective of the JTRS Step 2B Program awarded to Harris is to validate the SCA for man-portable, battery powered platforms. While these platforms are constrained by size, weight, and power, they often require increased performance for system turn-on time, system reconfiguration time and multi-channel operation. Because of this, man-portable, battery powered platforms have unique requirements that are different from those for larger vehicular, airborne and fixed station platforms.

5.1. Step 2B Program Approach

Harris performed the SCA validation effort by building the JTRS Manpack Test-bed Radio (JMTR) platform which, is based on the AN/PRC-117F (C) MPR, refer to Figure 5.1-1. The JMTR is a single channel radio which provides continuous, multiband frequency spectrum coverage from 30 MHz to 512 MHz and multi-mode operations for both LOS and BLOS UHF Tactical Satellite missions.

Figure 5.1-1 Step 2B Program JTRS Man-pack Testbed Radio

For the JTRS Step 2B program, Harris established an SCA compliant Operating Environment (OE), including development of a Core Framework (CF), platform device/service capabilities, and two separately developed JTRS compliant Waveform Applications. The OE and Waveform Applications were installed on the JMTR and presented to the JTRS JPO through a series of increasingly capable demonstrations. The JMTR platform was updated with new digital processing technology, including Harris Sierra™ devices in order to support full SCA V2.2 requirements (security).

Separately, Harris also ported the SCA V2.2 operating environment and waveform applications to a single channel, 30 – 512 MHz, fully Type I secure JTRS Hand-held (HH) radio (refer to figure 5.1-2). Harris demonstrated this JTRS HH radio to the Government for full interoperability with the JMTR and multiple legacy radios. Productization of this fully secure JTRS HH Radio is currently

Figure 5.1-2 JTRS Hand-held Radio

underway at Harris including the NSA certification process.

Harris developed two waveform applications for the validation. The first waveform application developed was VHF/UHF Line-Of-Sight (LOS) waveform application supporting either Plain-Text (PT) or Cipher Text (CT) Continuously Variable/Slope Delta (CVSD) digital voice. The CT operating mode utilized KY-57 encryption. A 16kbps Frequency Shift Key (FSK) modem was used that operates over the 30 to 512MHz MHz frequency range.

For the second waveform application, Harris developed a Mil-Std-188-181B waveform application for UHF Dedicated SATCOM operation. This included PT and CT data operation at rates of 4800bps, 19.2kbps, 32kbps, 18.4kbps and 48kbps using Continuous Phase Modulation (CPM). The CT operating mode utilized KG-84 encryption. This provided a much more processing intensive waveform application for the validation effort.

In April 2001, Harris completed the first ever over-the-air JTRS waveform demonstration. This demonstration included successful VHF/UHF LOS digital voice communications between a JMTR running the Harris JTRS software and legacy radios. In October 2001, Harris demonstrated successful data communications with the AN/PRC-117F (C) MPR using the Mil-Std-188-181B waveform over a UHF TACSAT channel simulator. **In June 2003, Harris demonstrated the first ever over-the-air JTRS SCA security supplement compliant secure communications.** This demonstration used the VHF/UHF LOS waveform application with digital voice and KY-57 encryption, between the JMTR, the Harris JTRS HH radio and other secure legacy radios.

In September 2003, a JMTR was delivered to the Government JTRS Test and Evaluation Laboratory (JTeL) to be utilized as one of four identified Representative Hardware Platforms (RHW) for JTRS waveform testing and certification. The JMTR is the only battery powered RHW.

5.2. Step 2B Program Results and Observations

A series of validation tests were executed as part of the Harris Step 2B Program in order to measure and analyze the performance of the JMTR, as well as compare it to legacy systems. The following tables provide performance data collected during the Harris Step 2B Program, including INFOSEC. Table 5.2-1 provides a timing performance comparison between a legacy AN/PRC-117F (C) radio, the initial JMTR running the Harris Step 2B JTRS software without INFOSEC and the current JMTR running Harris Step 2B software with INFOSEC. Note that the measurement data has been normalized to the performance of the legacy radio.

Table 5.2-2 provides a memory storage capacity comparison between the JMTR running the Harris Step 2B JTRS software (with and without INFOSEC) and a legacy AN/PRC-117F (C) radio. Note that the measurement data has been normalized to the memory capacities of the legacy radio.

Measurement	Legacy Radio	Initial JMTR	Current JMTR
Power-up	1	8	2
Application switch time	1	16	2
Parameter change time	1	4	9
TX/RX turnaround time	1	3	12

Figure 5.2-1 Timing Performance Comparisons

Measurement	Legacy Radio	Initial JMTR	Current JMTR
ROM	1	2.0	2.0
RAM	1	1.5	3.0

Table 5.2-2 Memory Storage Comparison

5.3. CF-Lite

The SCA V2.2 compliant CF developed by Harris was optimized for battery-powered platforms, and is referred to as CF-Lite. These optimizations are intended to conserve platform processing power and storage requirements, in order to reduce critical system power-up and application switching times to usable levels, while maintaining the integrity of waveform application interfaces (and therefore ensuring waveform portability). The platform services and devices interfaces (known as Application Programmer Interfaces – APIs) specified by the SCA API supplement are preserved. It is essential that the SCA API supplement definitions are consistent with waveform application requirements. Since the majority of JTRS waveform applications are being developed in conjunction with Cluster 1, the services and device definitions must be propagated into the SCA standard and converge with the API definition work being done concurrently by the OMG Software Radio Domain Special Interest Group (DSIG).

Power-up and application switch times, as well as memory storage capacities are significantly impacted by the use and performance of the eXtensible Markup Language (XML) to describe system and software component characteristics. XML files are parsed both at system start-up time and during the waveform instantiation process. The XERCES XML parser alone consumes about 1.3Mb of program space (per parser), with the Domain Object Model (DOM) requiring approximately 10 bytes of storage per bye of XML. The overall XML content for JTRS platforms will be large, estimated at over 100,000 lines in support of ORD waveform requirements. The CF-Lite pre-parses XML on waveform application installation (local or over-the-air) and stores the information in a significantly more concise and efficient format, improving the performance of platform power-up and application switch times.

6. OPTIMIZING SOFTWARE EFFICIENCY

"Meeting battery-life and performance challenges"

Optimizing software efficiency is essential to meet challenging battery life and operational performance requirements of small JTRS platforms. While Moore's Law provides benefits in terms of increasing processing performance and packaging density, power utilization and thermal dissipation challenges are exacerbated by the former improvements. The previously described CF-Lite provides increased software efficiency for radio power-up and application switching time, several other software efficiency techniques must be employed in conjunction with the CF-Lite, such as: chip level power management, high efficiency waveform image storage, waveform component caching, use of optimized CORBA transports and application of emerging Cognitive Radio techniques.

Chip level power management involves taking advantage of hardware component specific power savings capabilities such as: processor sleep modes and active power management (i.e., Harris Sierra™). High efficiency waveform image storage facilitates much more rapid movement of data between non-volatile memory storage and dynamic execution memory. Due to the large size of the waveform application executable images, significant time can be consumed copying information through the SCA file system. Optimizing the internal storage representation of waveform application executable images allows the use of high performance memory copies.

Individual components of waveform applications are loaded from non-volatile storage into dynamic execution memory upon waveform instantiation. When mission operations require waveform switching on a particular radio channel, the teardown of the previous operating waveform's components are effectively unloaded from memory and the newly selected waveform's components are subsequently loaded into dynamic execution memory. There are many components which are common across selected waveform applications and therefore the re-loading of these components into dynamic memory represents unnecessary latency. In order to improve software loading efficiency, common components across waveforms can be cached in memory through more intelligent CF operations.

CORBA transports using TCP can introduce unpredictable latencies into CORBA invocations, negatively impacting real-time system performance requirements. Process co-location and custom transports can be employed to reduce CORBA latencies, using information transfer methods such as shared memory. As an alternative to developing custom CORBA transports, the Object Management Group (OMG) is developing a predictable transport solution for real-time systems using Pluggable Protocol technology. The Object Management Group (OMG) is evaluating the Extensible Transport Framework (ETF) Request for Proposal (RFP) <mars/03-02-01> that describes the use of Pluggable Protocol technology for reliable CORBA transports as an extension to the Real-Time CORBA specification.

Cognitive Radio techniques to provide higher efficiency operations based on actual radio platform usage. These techniques include radio behavior modification based on learning operator waveform selection choices. Radio behavior modifications can be used to further optimize caching of waveform components. As other Cognitive Radio techniques evolve, such as spectrum access control and utilization, these capabilities can be provided as future software upgrades for improved radio system performance for the war-fighter.

7. CONCLUSIONS

"Take Away Messages"

Harris is a key player in the military SDR industry, a multi-level JTRS participant, including a leader in the development and delivery of secure, battery-powered platforms. Harris Sierra™ technology provides a fully capable security solutions optimized for an unmatched combination of small size, high performance throughput (ie., WNW) and power management. Battery-powered platforms require increased software efficiency through multiple techniques to meet challenging battery life and performance requirements.

8. REFERENCES

[1] Brooks, F. P. Jr. "No Silver Bullet: Essence and Accidents of Software Engineering", Computer 20, April 1987

[2] Frauenfelder, Mark, "The Care and Feeding of Your Cognitive Radio", TheFeature, May 21, 2003.