Introduction

Electronic Countermeasures (ECM) encompass several types of systems, one of which is a jammer. A jammer is a device that emits RF energy to disrupt sensor signals, such as RADAR, or communication signals used by an enemy. Jammer systems range from simple noise emitters, such as barrage jammers, to more sophisticated systems such as deception repeaters. A growing area of interest is the Counter-IED application that jams communication signals used to activate improvised explosive devices (IEDs).

A reference design for a generic jammer system that can be used to detect, lock onto and jam threat signals emitted by an enemy is shown below. A jammer system typically works in conjunction with an electronic support measures (ESM) system that performs wideband spectral analysis and direction finding to identify threat signals. In addition, the jammer may target a single frequency band, jamming all threat signals within that band, or it may employ a search strategy where the RF front end will step through a larger frequency band in a pre-defined manner.

Jammer Application

Processing in a jamming system is generally broken into four sections: RF conversion, IF conversion, spectral analysis, and channel processing.

RF Conversion

The RF conversion section downconverts a wideband signal from RF to an IF for digitization using an analog-to-digital converter (ADC), and also to upconvert the output of a digital-to-analog converter (DAC) to the transmit RF frequency. Transmit and receive elements within the RF Conversion section are gated with a transmit/receive switch to support “look through” or “blanking”, allowing shut down of receiver functions during jammer transmission. This gating function may also be distributed across multiple channels when jamming is employed over multiple bands.
**IF Conversion**

The IF conversion section provides wideband analog to digital conversion for the receive signals and digital to analog conversion for the jamming signal. In addition, the converted data from the receive channel is time-stamped to allow synchronization of threat signals with the time of day. The IF Conversion block interfaces directly to the spectral analysis and channel processing sections.

**Spectral Analysis**

The spectral analysis section is used to allow a “fast follower” approach, allowing the system to detect active signals in the target band. This is typically done using a large FFT with windowing function and follow-on processing to identify the exact center frequency and bandwidth of the target signal. The detected signals of interest are then reported to the operational control section.

**Channel Processing**

Once signals of interest have been identified by the spectral analysis section, the channel processing section is then used to more closely examine the signals of interest. It is then used to correlate these signals against the current threat database, or user input, to identify active threat signals. If a threat signal is identified, the operational control section may command the channel processing section to generate a jamming signal that is then sent out through the IF and RF conversion sections.

**System Considerations**

The latency between the time a signal is detected and the time that the jammer signal is transmitted must typically be very small to provide effective jamming of short-duration or frequency-agile signals. Hence the spectral analysis function must be implemented in such a way to have very low latency. There is a tradeoff between the length of the FFT and the latency as longer FFTs provide better frequency resolution but require a longer time window to operate. The use of a digital downconverter before the FFT enables the system to select a narrower bandwidth of interest. This allows a shorter FFT while keeping good frequency resolution and improved overall system latency, albeit for a narrower band. Implementing the spectral analysis function in an FPGA allows fast FFT processing and also allows the analysis function to be tailored to the threat environment.

Coordination of these four processing sections is facilitated through an operational control element consisting of a finite state machine (FSM) and a number of control ports. This control element typically maintains the threat database, and is used to dynamically load and unload jamming modulation schemes. In addition, when used in conjunction with ESM systems, the operational control element must provide a gating mechanism to these other systems to coordinate “look through”.

**Implementation on Spectrum’s SDR–4902**

The SDR-4902 provides a hardware platform to implement the RF conversion, IF conversion, spectral analysis and channel processing functions outlined above. The SDR-4902 is a two card, 3U CompactPCI subsystem that covers the frequency band ranging from 200 MHz to 2.7 GHz. The subsystem consists of the RF-4902 Wideband RF-to-Digital Transceiver card, and the PRO-4600 Baseband Processor card.

![Figure 2. RF-4902 Transceiver Card](image)

![Figure 3. PRO-4600 Processor Card](image)

The RF-4902 features a 14-bit 490 MSPS ADC, a 16-bit 980 MSPS DAC, and a Xilinx Virtex-5 SX95T-2 User FPGA. The PRO-4600 is equipped with an MPC8541e general purpose processor (GPP), a TI C6416T DSP, and a user programmable Xilinx Virtex-4 LX60 FPGA. The two cards are closely coupled by means of a SPI control interface, high speed serial data interface, and additional GPIO and interrupt lines.
In this example, the RF conversion and IF conversion sections are implemented in the RF-4902 hardware as seen in Figure 4.

The spectral analysis and channel processing functions are implemented in the RF-4902 User FPGA. Threat and jamming signal parameters are stored on the RF-4902 transceiver in the local SDRAM associated with the FPGA processor, minimizing the latency associated with each "look up" of this data. Time-stamping of received signals is supported through the 1PPS interface, and coordination of gating for multi-channel "look through" is supported through a front or rear panel GPIO connector. The User FPGA on the RF-4902 provides for the spectral analysis section, with support provided for up to a 32K point FFT while maintaining real-time performance. Wideband signals can be captured to the SDRAM onboard the RF-4902 User FPGA to enable uploading to a host for later analysis. Operational control of this system is distributed, with local control on the RF-4902 User FPGA and subsystem control on the PRO-4600 GPP. Additional signal processing elements are available on the PRO-4600 as needed.

The RF-4902 has a wide bandwidth that enables hop following for a jammer system. The spectral analysis section detects the RF signal anywhere within a wide bandwidth, for example, 100 MHz, and steers a jamming signal to the desired frequency to be jammed.

The DDC and spectral analysis functions can be implemented using rapid development tools such as MATLAB, Simulink, and Xilinx System Generator. Example implementations of DDC, DUC and spectral analysis functions are available with the SDR-4902. These examples are implemented using the tools mentioned above and are provided so users can easily modify them to suit their requirements.
Conclusion

This application note outlines how a jammer can be implemented on the SDR-4902. If you have questions about this application note, or other applications that Spectrum can help realize, please contact Spectrum’s sales and applications staff.

Sales: sales@spectrumsignal.com
Tech Support: support@spectrumsignal.com
Tel: 1.800.663.8986 (toll free North America) or +1.604.676.6700 (international)
Web www.spectrumsignal.com