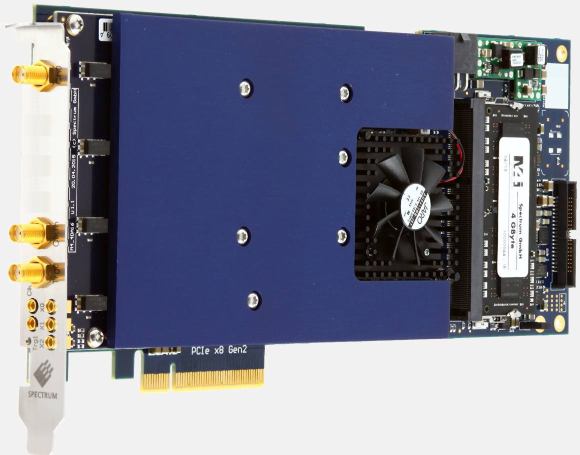
Application Note

Characterization of Remote Keyless Entry device

Using Modular Digitizers for Physical Level Characterization of Remote Keyless Entry devices

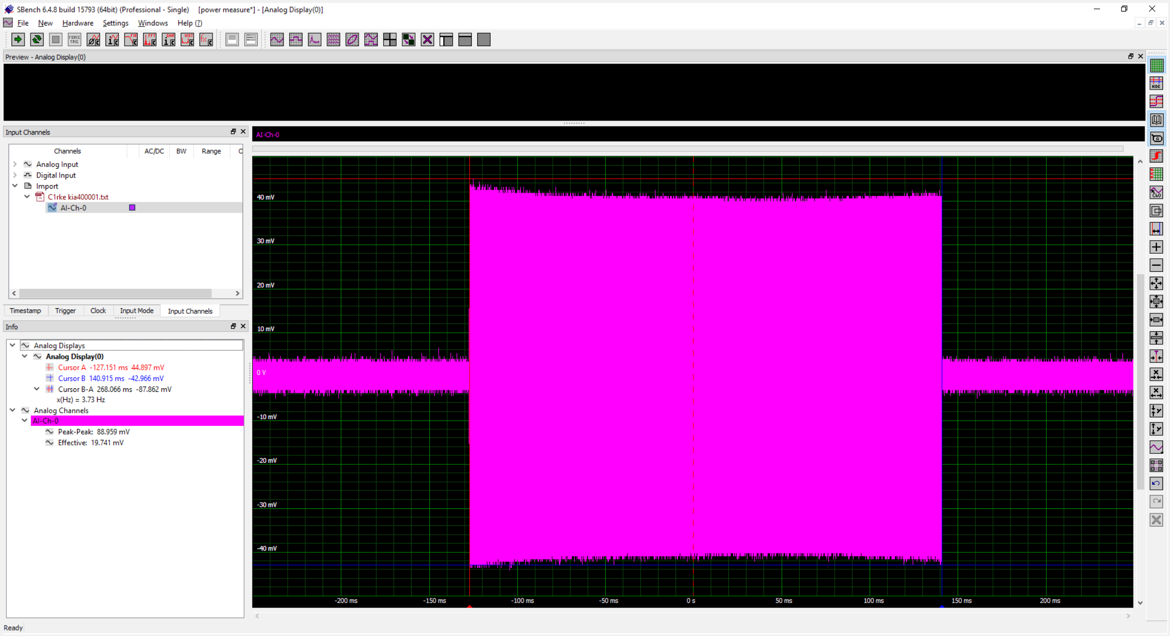
Automotive technology is packing more functionality into every device. Consider the vehicle key fob, it has evolved from a simple mechanical key to a miniature electronics power house, incorporating remote key entry (RKE), remote starter, and keyless ignition. Remote key entry and remote starter use an ultra-high frequency (UHF) transmitter employing intelligent encoding to maintain security. Design verification and testing of the physical layer operation of these devices requires tools that can acquire and measure the RF signals of relatively long duration and do further processing to extract additional information. Modular digitizers are ideal measurement instruments for RKE measurements, a study of typical RKE measurement parameters will reveal the specifications required to select an appropriate modular digitizer.



The Spectrum M4i.2230-x8 8 bit 5 GS/s PCIe digitizer is used to acquire the RKE signals

RKE devices operate in the industrial, scientific, and medical (ISM) frequency bands which allows unlicensed low power radio transmission. The nominal frequencies used are 315 MHz and 433.92 MHz in the United States and Japan and 434.79 MHz and 868 MHz in Europe. The carriers of these radio signals are binary modulated by either amplitude shift keying (ASK) where the amplitude of the carrier is varied between two levels or Frequency Shift Keying (FSK) where the frequency of the carrier jumps between two distinct values. The protocol used for transmitting data to the vehicle are proprietary to each manufacturer. In general, the data packets consist of from 64 to 256 bits transmitted at from 1 to 20 kilobits per second (kbps). The packets include a preamble, command code and a rolling code. The command code segment of the data packets controls access to the vehicle. This usually includes commands to lock and unlock doors, start the engine, and turn on the emergency alarm. The rolling code is a security feature that assures that the same code is not sent out with each use. The RKE module or fob communicates with the vehicle via the body control module (BCM) which controls the electromechanical devices within the vehicle.

A typical data packet transmitted from an RKE fob is shown in Figure 1. The packet was a near field acquisition over the air. Its duration is 269 ms as measured with cursors with the readouts shown in the information pane on the lower left. The carrier frequency is known to be 433.92 MHz. This combination of relatively high frequency carrier and long duration makes this measurement challenging for many instruments.



Analog Displays
Analog Display(0)
Cursor A -127.151 ms 44.897 mV
Cursor B 140.915 ms -42.966 mV
Cursor B-A 268.066 ms -87.862 mV
x(Hz) = 3.73 Hz
Analog Channels
AI-Ch-0
Peak-Peak: 88.959 mV
Effective: 19.741 mV

Figure 1: A typical RKE packet. It has a duration of 269 ms as read by the measurement cursors. The peak to peak amplitude is 89 mV and the effective or RMS amplitude is 19.7 mV as read using the measurement parameters displayed in the 'Info' pane.

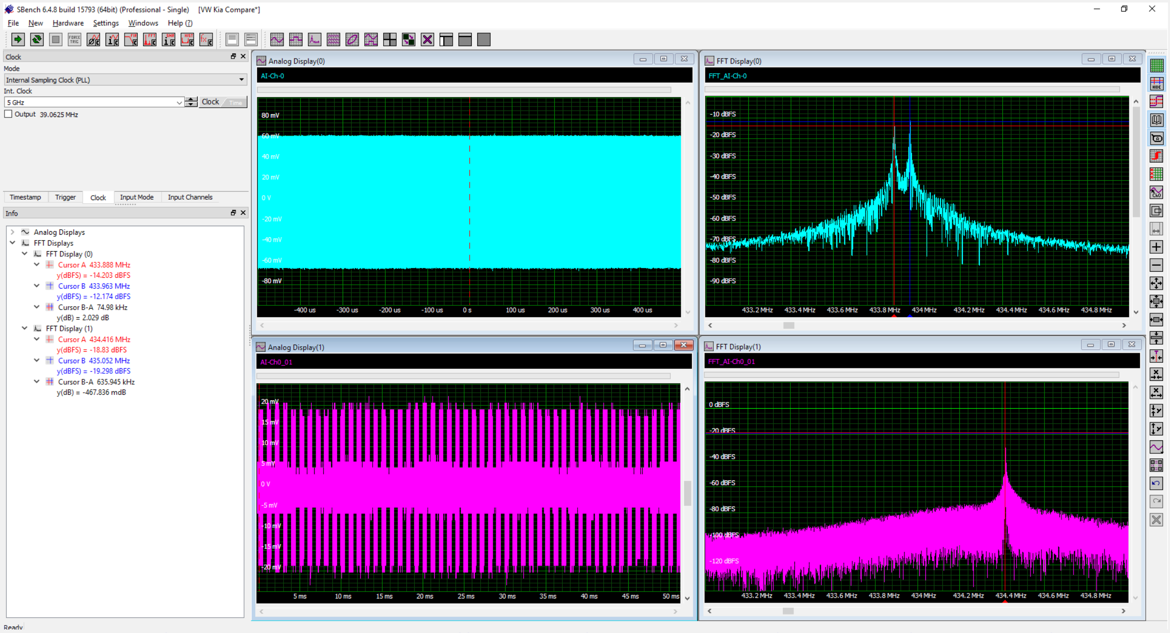
An instrument used to acquire this waveform has to have a bandwidth greater than the carrier frequency. Since bandwidth is generally defined as the half power or -3dB point in the instrument's frequency response the usual practice is to select an instrument with twice the signal's bandwidth in order to assure operation in the flattest part of the instrument's frequency response.

The sampling rate of the measurement instrument must be greater than twice the signal's bandwidth. So, for a narrowband 433.92 MHz carrier the sample frequency has to be at least 868 Mega Samples per second (MS/s). Instruments, such as the digitizer used for this example, offer sampling rates that are in binary steps starting at 5 GS/s so sample rates of 5, 2.5, or 1.25 GS/s could be used as they all exceed twice the clock frequency. Sampled at 5 GS/s the 269 ms duration would require 1.345 Giga Samples (GS) of memory. Sampling at 1.25 GS/s would require 336 MS. The example in Figure 1 was acquired on a Spectrum Instrumentation model M4i.2230-x8. This is a single channel, 8-bit digitizer with a 1.5 GHz bandwidth, 5 GS/s maximum sample rate, and 4 GS of acquisition memory. A 4 GS memory can acquire 800 ms of data at a sampling rate of 5 GS/s. This provides good time resolution which is helpful in interpreting phase or frequency modulated signals. Modular digitizers also offer multiple acquisition modes that are intended to use acquisition memory efficiently and decrease the dead time between acquisitions especially with signals that occur at a low duty cycle.

From an amplitude perspective, this digitizer has a minimum input range of ±200 mV full scale with an optional low voltage range of ±40 mV full scale which are well matched to the signal amplitude of 89 mV peak to peak read using a direct analog measurement parameter in the software. The input impedance is 50 Ω consistent with the digitizer's 1.5 GHz bandwidth.

The software used to display the acquired RKE data is Spectrum Instrumentation's SBench 6 measurement software. This software is a powerful and instinctive interface that allows acquisition and measurement without the need to write code to program the digitizer. It also includes a broad range of measurements and signal processing tools to evaluate the RKE type devices as well as many others.

These tools include automatic measurements of acquired signal, Fast Fourier Transform (FFT) for spectrum analysis, and filtering. As an example, Figure 2 shows a comparison of two different RKE fobs using the M4i.2230-x8 and SBench 6.



SBench 6.4.8 build 15793 (64bit) (Professional - Single) [VW Kia Compare*]

Clock

Mode: Internal Sampling Clock (PLL)

Int. Clock: 5 GHz

□ Output 39.0625 MHz

Info

- Analog Displays
- FFT Displays
  - FFT Display (0)
    - Cursor A 433.888 MHz
      y(dBFS) = -14.203 dBFS
    - Cursor B 433.963 MHz
      y(dBFS) = -12.174 dBFS
    - Cursor B-A 74.98 kHz
      y(dB) = 2.029 dB
  - FFT Display (1)
    - Cursor A 434.416 MHz
      y(dBFS) = -18.83 dBFS
    - Cursor B 435.052 MHz
      y(dBFS) = -19.298 dBFS
    - Cursor B-A 635.945 kHz
      y(dB) = -467.836 mdB

Figure 2: Waveforms acquired using two different RKE fobs. The upper left trace uses frequency shift keying, The FFT of this waveform in the upper right show's dual spectrum peaks. The fob shown in the lower left trace uses amplitude shift keying has a single spectral line in the FFT with broad sidebands.

The trace on the upper left grid uses frequency shift keying (FSK). The carrier shifts between two frequencies to indicate the binary state '0' or '1'. This can be seen on the FFT in the upper right grid. The frequency spectrum has two spectral lines. One at 433.89 MHz and the other at 433.96 MHz as indicated by the cursor readouts, they are symmetrically spaced 70 kHz apart about the nominal 433.92 MHz carrier frequency. The FFT function allows the digitizer to act like an RF spectrum analyzer showing the frequency or spectral view of the waveform but without requiring a separate instrument.

The RKE fob signal, shown in the lower left grid, uses amplitude shift keying (ASK). The binary data modulates the amplitude of the carrier resulting in a signal envelope showing rectangular pulse shape. The FFT of the ASK signal has a single spectral peak at the carrier frequency of 434.41 MHz.

Further analysis of these RKE signals is possible using the signal processing tools available in SBench 6. It is possible to demodulate both of these types of signals as shown in Figure 3.

Application Note

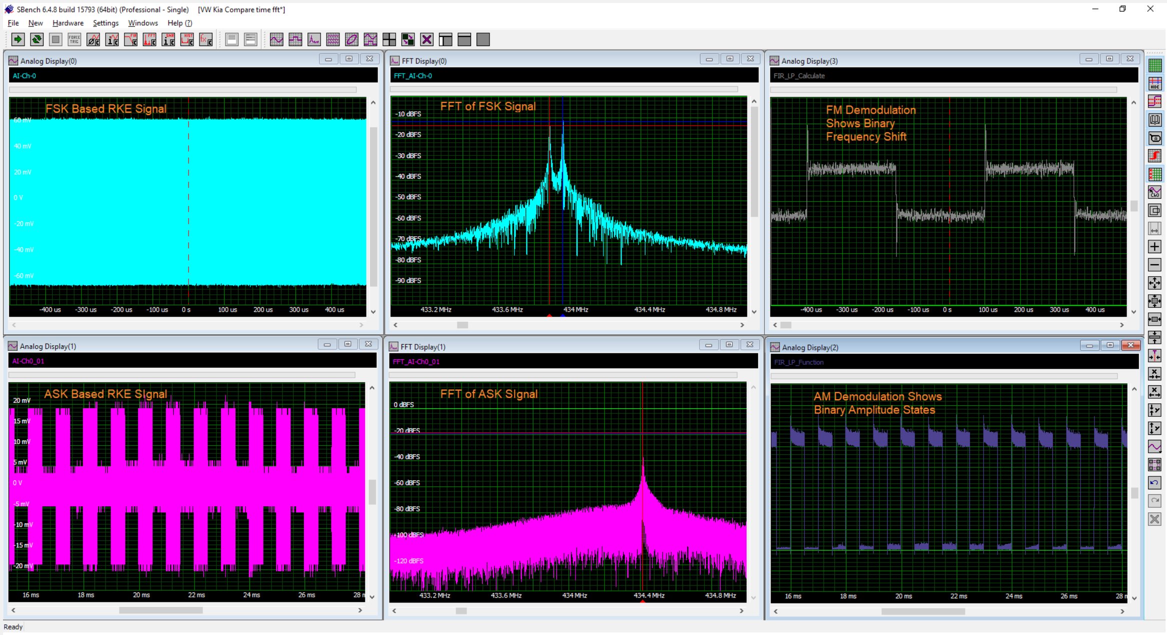
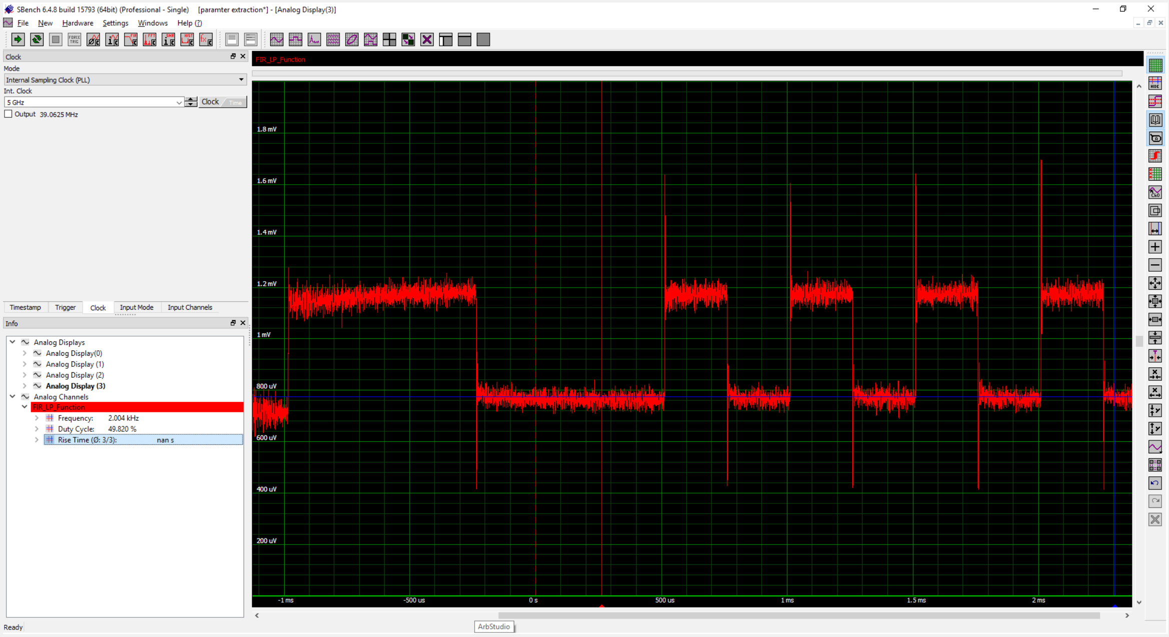


Figure 3: Using the signal processing tools in SBench 6 the RKE signals can be demodulated to verify key data related parameters such as data rate.

The ASK signal can be demodulated by multiplying the signal by itself, thus squaring it, and then low pass filtering the result. This essentially performs RMS detection. This is shown in the lower right grid in the figure.

Demodulation of the FSK signal is accomplished using slope detection. The signal is passed through a high pass filter. The filter frequency response is selected so that the frequency shift of the carrier sits on a slope of the filter frequency response. This results in the different frequencies being translated into a differences in amplitude. This, now amplitude modulated signal is demodulated using the same RMS detection process outline earlier. The result is shown in the upper right grid in the figure.

Demodulating the RKE signal enables determination of the physical characteristics of the modulation, such as the data rate, duty cycle, rise time, and related timing measurements can be measured. The example shown in Figure 4 shows the demodulated data from an FSK based RKE fob. The data is measured between the cursors and includes the four pulses on the right of the display.



SBench 6.4.8 build 15793 (64bit) (Professional - Single) [paramter extraction*] - [Analog Display(3)]

Clock

Mode: Internal Sampling Clock (PLL)

Int. Clock: 5 GHz

□ Output 39.0625 MHz

Info

- Analog Displays
  - Analog Display(0)
  - Analog Display (1)
  - Analog Display (2)
  - Analog Display (3)
- Analog Channels
  - FIR_LP_Function
    - Frequency: 2.004 kHz
    - Duty Cycle: 49.820 %
    - Rise Time (Ø: 3/3): nan s

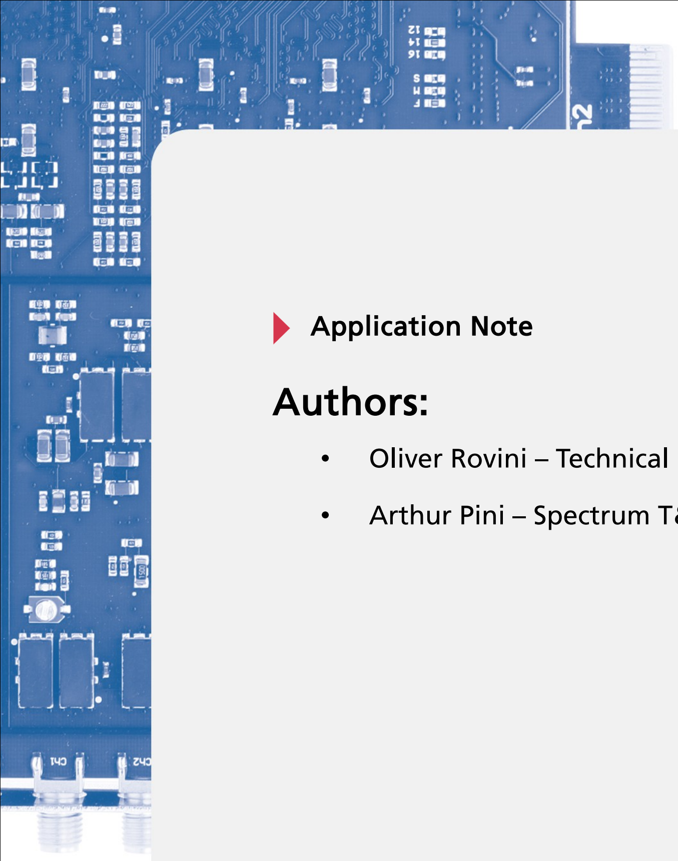
Figure 4: Measurements made on the demodulated FSK signal include the frequency, duty cycle, and rise time. The measurements are gated by the cursors and include only the four pulses on the right of the display.

The data rate of the pulses is 2 kHz, the duty cycle is 49.8% and the rise time is 602 ns. This information is vital when troubleshooting a problem and it is not apparent from the raw FSK modulated carrier.

Still more sophisticated data analysis can be achieved using third party software such as MATLAB or LabVIEW or even custom programming in C, C++, or Python. These third-party programs offer the ability to decode the data packets rapidly. Because these programs can be customized, they offer great flexibility and allow much more analysis, including protocol decoding. This capability for processing outside of the digitizer is enhanced by the M4i.2230-x8 digitizers PCI Express x8 Gen 2 interface. This interface, using Spectrum's drivers can achieve data transfer rates of greater than 3.4 GB/s with suitable host computers. This transfer rate is very essential when dealing with waveforms like these that are hundreds of MB long as it allows rapid transfer of the data to the host computer.

Even greater processing power is available for those with intermediate level programming skills, in the form of the Spectrum CUDA access option for parallel processing (SCAPP) which allows a direct connection between the digitizer and a CUDA based graphics processing unit (GPU). This makes the GPU's multiple processing core and super-large memory available for advanced high-speed signal processing. In this application it can provide significantly faster filter and FFT calculation times.

High frequency modular digitizers like the Spectrum Instrumentation M4i.22xx series are ideal instruments for testing RKE or related active radio frequency identification devices (RFID), which share the same UHF frequency spectrum assignments. They involve high frequency carriers modulated at relatively low digital data rates requiring extremely long acquisitions at high sample rates. The digitizers have 1.5 GHz bandwidths compatible with the devices being tested. They include 5 GS/s maximum sampling rates with 4 GS long acquisition memories to capture full data packets at the highest sample rates. This acquisition engine is backed by a 3.4 GB/s PCI Express bus to move the data quickly to a host computer for fast analysis and data archiving. A well-matched application and instrument combination.



Authors:

- Oliver Rovini – Technical leader of Spectrum Instrumentation, Germany
- Arthur Pini – Spectrum T&M engineer, USA