PCARA Update

Have some Pi

[N.B. This article was composed using a Raspberry Pi 3 Model B+]

The February PCARA Breakfast on the 16th was attended by 14 members, including some we haven't seen in a while. As always we had a wonderful time with much conversation and laughter. Unofficial business was discussed as well as ideas for club activities going forward. If you've not had the opportunity to join us,

PCARA Breakfast on Saturday Feb 16.

please consider doing so. ALL ARE WELCOME. I promise, you will not be disappointed. Our next **PCARA Breakfast** will be on March 16, 2019 at 9:00 a.m. at Turco's in Yorktown Heights, NY. [Just after Pi-Day, 3/14 -*Ed*.]

If the idea of an enjoyable breakfast isn't enough of an incentive to come out on a Saturday morning, perhaps a **PCARA V.E. Test Session** will be. At 11:00 a.m. on March 16, 2019, PCARA will be sponsoring a V.E. Test Session at the John C. Hart Memorial Library in Shrub Oak, NY. If you know of anyone who might be interested in taking an exam, please invite them to join us.

PCARA has reserved a table at the Orange County Amateur Radio Club (OCARC) **Spring Hamfest** on Sunday April 28, 2019 at the Town of Wallkill Community Center, 2 Wes Warren Drive in Middletown, NY. Members are encouraged to bring along items they wish to sell and place them on the table. This might provide an opportunity for beginning the spring cleaning that your shack so sorely needs. Please join us.

A **PCARA Foxhunt** has been officially scheduled for Saturday May 11, 2019 — *CQ Magazine* Foxhunt Weekend. Due to his talent as the Fox during the previous PCARA Foxhunt and not being found, Mike N2EAB has once again earned the honor of being hunted again. Rules and further details to follow. Also, the suggestion of a 440 MHz Simplex Challenge in April has been

made — most likely on Saturday April 13th. Stay tuned and start work on those 440 MHz Yagis now.

Lou KD2ITZ entered PCARA into the Icom America Club Net Contest to try and win some Icom swag, and we did! PCARA was chosen as a 2019 – Segment 1 Monthly Winner. The swag kit includes an Icom Ham Crew T-shirt, water bottle, hat, and backpack. To see the winning announcement please visit: https://www.icomamerica.com/en/amateur/club-net/winners.aspx. **Thanks Lou!** When the prizes come in we'll raffle them off at the next monthly meeting.

Talking about meetings, our next regularly scheduled membership meeting is on Sunday March 3, 2019 at 3:00 p.m. at New York–Presbyterian / Hudson Valley Hospital in Cortlandt Manor, NY. I look forward to seeing each of you there. - 73 de Greg, KB2CQE

Contents

PCARA Board

President:
  Greg Appleyard, KB2CQE; kb2cqe 'at' arrl.net
Vice President/Treasurer:
  Joe Calabrese, WA2MCR; wa2mcr 'at' arrl.net
Secretary:
  Lou Cassetta, KD2ITZ, radiocassetta 'at' gmail.com
Directors:
  Bob Tarsio, N2CBH
  Mike Dvorozniak, W2IG

Net night

Peekskill/Cortlandt Amateur Radio Association holds a weekly net on the 146.67 MHz W2NYW repeater on Thursdays at 8:00 p.m.

Join net control Karl, N2KZ for news and neighborly information.

Adventures in DXing

- N2KZ

Got Your Number

The world of ham radio seems to be obsessed with numbers. A majority of operators only get on the air when there is something to achieve. Who will work the most countries, states, districts, counties, cities, Maidenhead grids and a myriad of other things? Did you get your consecutive number from the other station? Make sure you don't negate your entry with incorrect data!

There is a lot of planning to do. Do you have and understand the contest rules? Will your social and work schedules be free for the duration of the contest? Have you tested all of your equipment for proper operation? Is your logging software up and running? Are your antennas in good working order?

Let's talk about the practical aspects: How close is your shack to the nearest bathroom? Do you have plenty of coffee on hand? Is there someone nearby who can feed you and get you drinks? When will you sleep? (Who sleeps?) Will your wife, girlfriend or friends understand? (Will they *ever* understand?)

Your memory keyer or voice recorder is programmed. You have a comfortable chair and headset. You have sufficient light for overnight operation. Dreams of instant gratification will soon become reality! Your fascination with numbers is about to be fulfilled! The anxious anticipation of achieving great things is now almost unbearable! (Your psychiatrist lowers their glasses and asks... 'So when did this all start?')

Figure This

I first encountered the numbers game around 1965. This was the year I began listening to a wideband (500 kHz to 30 MHz) radio. I always kept casual notebooks to recall the stations I heard. I wrote away for QSLs from shortwave broadcasters all over the world. Remember 'International Reply Coupons' used as return postage? It was a casual hobby that really held my interest.

It wasn't long before I created a schedule for myself to listen to a continual stream of overseas programs. It was an interesting backdrop during those endless hours of school time homework and study. I could visit Holland, Switzerland, Britain, Sweden, Spain, Portugal and even Israel and Egypt almost every night. What a magical thing a shortwave radio can become!

Part of my indoctrination to the shortwave listening hobby was reading magazines like *Popular Communications*, *Communications World* and *White's Radio Log*. I began to understand the many levels of achievement to consider. How many countries have you heard? Have you logged interesting places like India, Japan and New Zealand? Did you hear the special event station last weekend?

I sent questions to listener clubs like 'Sweden Calling DXers.' I joined established organizations like the Radio-Canada Shortwave Club. Visiting the CBC in Montreal in 1967, I even met CBC radio personalities like Ian McFarland, Pip Duke, Elaine McMaster and Duncan Nicholson. Indeed, it was quite a hobby!

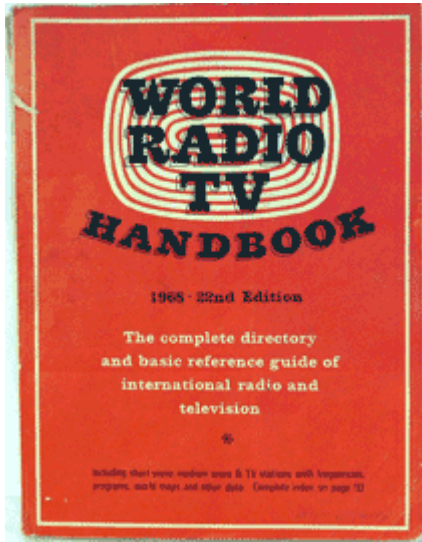Fear not! There were lots of frequency numbers to remember on shortwave too: Australia in the morning on 9580, the BBC on 9410 or 15070, CBC Northern Service on 9625 and ever-present CFCF/CFCX

Karl's Certificate of Membership for the Radio Canada Shortwave club.

Montreal on 6005. Switzerland on 9725, Sweden on 9695, Ghana on 6130. The Far East would always include the fluttery sound of double-hop skip propelled by enormous transmission power trying to bring their signals to North America during American evening after-dinner prime time. Radio Peking, Radio New Zealand, Radio Japan and Radio Australia all pumped megawatt signals onto 19 meters and

Radio Australia ad in WRTH, 1965.

even 16 meters after dark. How could you learn about this myriad of numbers? One of the nicest presents you could ever receive was a book just *filled* with numbers: The encyclopedic *World Radio TV Handbook*!

WRTH 1968 - 22nd Edition.

Numbers continued to follow me... and elude me. I don't think I ever reached as far as 100 countries heard on shortwave. I don't think I ever heard 1000 different stations on AM radio and I know I never heard 100 *countries* on AM radio... but I met a lot of people who did!

You have to wonder about those who spend countless hours, days and years trying to obtain greatness and notoriety as a DXer. With any analytical skills at all, you might easily conclude that serious never-ending DXing is a manifestation of obsessive-compulsive disorder. I think I would use the word *determination* instead.

Keep Counting

Consider the time and effort needed to rise to the higher echelons of amateur's DXCC rolls. My good friend Bob Myers, K2TV, has logged 353 entities for his DXCC. Bob's achievement demonstrates his continual passion for our hobby over a period of nearly 60 years of operating! The ultimate goal may be unattainable. There is always one more country or island that you haven't worked. Like they say in the Pokémon world: 'Gotta catch 'em all!"

Medium wave DXers have shown me just how far they will dig for a new station. In the AM band, there are six 'graveyard' channels that host hundreds and hundreds of local stations: 1230, 1240, 1340, 1400, 1450 and 1490 kHz. Unless you just happen to have a local station on one of these frequencies close to your QTH, 'graveyard' channels sound reminiscent of CB trucker channel 19.

To pull station IDs out of the muck, many skilled and savvy medium wave DXers use their computers to record only top-of-the-hour station IDs automatically. Their audio recorders record a minute or two before and after 'straight up' so you don't have to listen to hours and hours of programming that will reap no results. Now you can survey a full day's legal IDs in just a few minutes! DXing 'graveyard' channels can become almost rational!

Other techniques include audio equalization, nulling and phasing multiple antennas together to create quite remarkable directional pickup patterns and using exalted carrier single sideband (ECSS) reception to eke out the most elusive catches.

Don't let the lingo scare you! ECSS simply means that you are listening to an AM signal using single sideband mode. This allows you to hear two renditions of one reception — both upper and lower sidebands. If one sideband is loaded with adjacent channel interference or an audio fade, the other sideband might be able to bring it through.

Ace DXer Patrick Martin of Seaside, Oregon agrees: "ECSS [Single Sideband] is about the only way I DX these days. It is much easier to pull an ID out of the jumble. That is one way my Drake R8 really "sings" in the ECSS mode. Many catches I would never have heard without it." Patrick has

Drake R8 communications receiver covers 10 kHz - 30 MHz.

one of the finest set of logbooks in the world of AM radio listening including stations from all over the Pacific rim, Asia, India and surrounds.

Although 'graveyard' broadcasters usually operate with 1000 watts or less, simply amazing receptions can happen. A miracle once occurred for another ace DXer Pete Taylor. While DXing in Hawaii, Pete pulled through a 'graveyard' station on 1230 kHz from Argentina about 7500 miles away!

With results like this, you might really want to consider spending some time with the 160 meter amateur band. Just think what you could catch *without* hundreds of stations on a channel! The frequencies

between 1800 and 2000 kHz are wide open and ready for your use. Go to them!

These higher medium wave frequencies (1500 to 2000 kHz) tend to be even more 'short-wavey' than lower broadcast medium wave, making them primed for long-haul DX. The best times to listen to the medium waves are an hour or two before and after local sunrise and sunset (known as gray-line propagation) and between the hours of about 1:00 to 3:00 a.m. in the wee hours of the morning. For instance, the only times I have ever heard KFI 640 kHz Los Angeles here in Westchester was at about 2:30 a.m. Give it a try!

Machine Replaces Man?

Digital amateur radio DXers in the year 2019 are transfixed by speed. The faster you can turn a QSO, the more QSOs and multipliers you can score per hour. (You can win contests that way!) Casual yet proficient contest operation should score you at least 30 QSOs an hour. Using the latest proper software, equipment peripherals and seasoned experienced contest techniques, you might likely exceed 100 QSOs an hour. Maybe its time to hang up your straight key and pencil-and-paper logbook!

Like most everything else in this modern age, the hobby is starting to lean heavily towards autonomous operation. Efficient human interaction, high transmit power, use of spotter sites and waterfall displays and automatic full-bandwidth tuning are now the name of the game. Voice recognition can now control properly fitted computer-based transceivers. (You don't want to waste precious time looking for a knob or button — or even worse — manipulating it!)

The hot mode of the moment is **FT8** — a truly astounding system of message communication. The underlying scheme behind FT8 was originally conceived to advance the challenging pursuits of moon-bounce and meteor scatter DXers. FT8 was designed to promote very weak signals in the worst environments. It can propagate during miserable conditions and allow quite marginal stations to flourish.

Take a listen to the fury of this mode. Simply tune to 3573, 7074 or 14074 kHz and listen in USB CW mode. The working bandwidth of FT8 is from these frequencies to +3 kHz, so tune slightly higher up to hear more activity. Amazed at how many signals you hear all at once? FT8 allows you to work many stations rapidly, near and far, within a nearly fully automated domain. Without much effort, setup your equipment, get on the air and may the DX begin!

If you are not quite ready to command a ham radio spaceship, you may want to venture into more pedestrian operation using good old-fashioned CW, now augmented and ready for use in the third decade of the 21st century! Although RTTY and PSK31 continue to be popular, you can also bang out CW at fast

Partial screen-shot of WSJT software in FT8 mode.

speeds without touching a traditional key or bug.

Using a keyboard to send your code — and — a software-based CW reader program like CWGet (https://www.dxsoft.com/en/products/cwget/) you can transmit and receive code without any knowledge of the dits and dahs of traditional Morse. Speeds of up to 50 words per minute are attainable. Most CW contest keyboard and reader operation hovers at about 25 words per minute. It is a wild world out there. What happened to good old CW, AM and SSB?

When a new mode becomes very popular, you have to expect naysayers. FT8 is designed to make rapid contacts exclusively. It removes all aspects of conversation and speeds along without any human interaction. FT8 can become quite boring and encourage complete operator burnout. But! It also increases your capability of logging tremendous numbers of QSOs by (maybe?) ten-fold! Also, keep in mind that modes like FT8 will always be continually further refined or modified as desired as time goes by. Have you ever seen a computer software package that remains static forever? What new mode will the future bring?

Revere the wisdom of the Greek philosopher Heraclitus: *The only thing that is constant is change.* Amateur radio operators will always be working to improve their designs, appreciate their achievements and increase their numbers. Count on it!

Heraclitus

My sincere thanks to my friends Malcolm, NM9J and Joe, WA2MCR, for their help and guidance in assembling this article. (P.S. I *still* like my straight key and pencil!) Until next month, 73 and dit dit de N2KZ 'The Old Goat.'

SDR Spectrum Analyzer – KD2ITZ

Invaluable instrument

A spectrum analyzer is an instrument that measures the magnitude of an input signal over a range of frequencies. Whereas an oscilloscope displays the magnitude of a signal against time, a spectrum analyzer presents data in the frequency domain — amplitude against frequency.
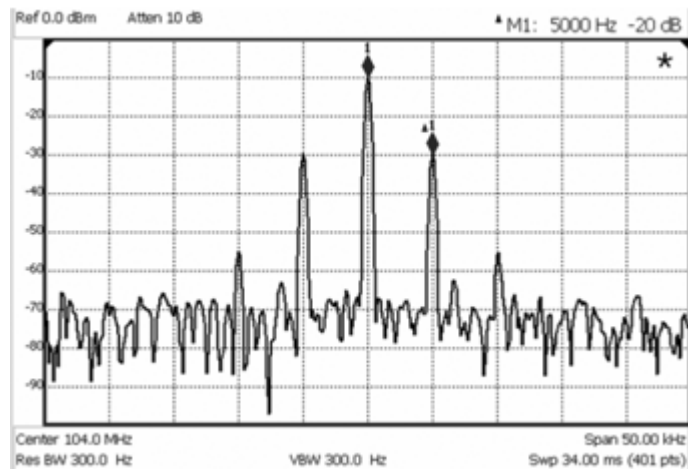

Figure 1. Keysight spectrum analyzer displaying amplitude vs. frequency. [keysight.com]

Spectrum analyzers are valuable in determining frequency response, noise and distortion in radio-frequency (RF) circuitry. The cost of professional-grade spectrum analyzers is prohibitive to most radio amateurs. Depending on frequency range, instruments from major manufacturers vary in price from $2,000 to over $40,000. Thankfully, there is a versatile alternative that costs several orders of magnitude less.

Keysight N9320B basic spectrum analyzer covering 9 kHz to 3 GHz costs $9,467.00.

SDR on a stick

Many readers may be familiar with USB dongles that function as **software defined radio** (SDR) receivers. Low-cost versions are readily available and were originally intended for TV reception in a format not used in North America: Digital Video Broadcasting — Terrestrial (DVB-T). Enthusiasts soon learned how to access the hardware's raw I/Q data and that these devices were capable of much more than TV viewing. With the development of free and open-source software, these dongles have been employed as receivers

and scanners for numerous applications. One of the major advantages of using a SDR is the ability to receive a signal and simultaneously view the presence of other signals on nearby frequencies through a spectrum scope. With the proper software, the SDR dongle can generate quantitative measurements of signal amplitude across a wide range of frequencies and function as a usable spectrum analyzer.
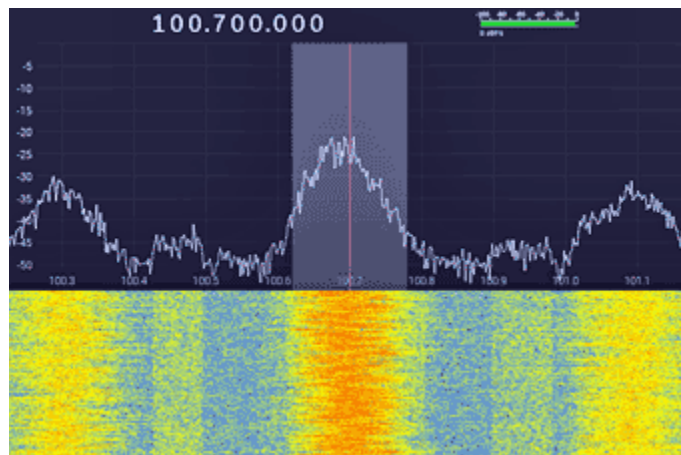

*Figure 2. SDR reception of FM broadcast using **gqrx** software, http://gqrx.dk/.*

An excellent source of information on SDR dongles is RTL-SDR, https://www.rtl-sdr.com/. Following the instructions on their site, I was able to experiment with free spectrum analyzer software and inexpensive hardware. I had already purchased a dongle on eBay in 2015. It contains a Realtek RTL2832U DVB-T demodulator chip and Rafael Micro R820T tuner. The 75Ω antenna input employs a MCX jack. The black plastic case provides no shielding. Similar devices cost approximately $8.00. The frequency range is reported to be between

Fig 3. RTL-SDR.com publishes free tutorials and also sells books and devices.

Fig 4. SDR Dongle. Search eBay for RTL2832U to find listings.

25 MHz-1750 MHz. Up-converters are available to receive frequencies below 25 MHz. Various other vendors sell dongles that include HF coverage and metal cases.

SDR dongle set-up

The SDR dongle was one of my first purchases as a new ham. When I tried to use it on my desktop PC, I quickly learned that RF interference from the PC power supply created difficulty receiving signals. In order to ensure accuracy for experimentation as a spectrum

analyzer, I used a **Raspberry Pi Model 3**. The single board computer can easily be battery powered, but I did not discern RF interference using an Enercell 1.5A power supply. Software drivers from Osmocom must be installed in order to use the dongle as a SDR. Included with this bundle is a program called **rtl_power**. It allows quantitative measurement of power levels across the entire frequency range of the device. It is run from the command line and outputs a data file in comma-separated values (CSV) format.

Raspberry Pi 3 single board computer.

Drawing the graph

This data can be graphed using spreadsheet software to resemble the output of a spectrum analyzer. Alternatively, a free program with a graphical user interface (GUI), called **RTL SDR Wide Spectrum Analyzer**, can be used to control rtl_power and view the data. Other spectrum analyzer programs with GUI's are also available. They may not be compatible, however, with a Raspberry Pi running Raspbian OS.

There are drawbacks with the experimental setup compared to a professional device. The amplitude of the signal on the Keysight spectrum analyzer in Figure 1 is measured in decibel-milliwatts (dBm). These values are referenced to one milliwatt and are absolute. The SDR reports values in decibels (dB), which have only relative value. Figure 5 shows artifacts arising from the device's local clock oscillator. Signal amplitude was measured from 26 to 176 MHz with a 50Ω dummy load connected to the antenna input. The peaks correspond to the fundamental and harmonics of the 28.8 MHz crystal frequency. There is also an unexplained saw-toothed wave at the baseline with an amplitude of approximately 3dB peak to peak.
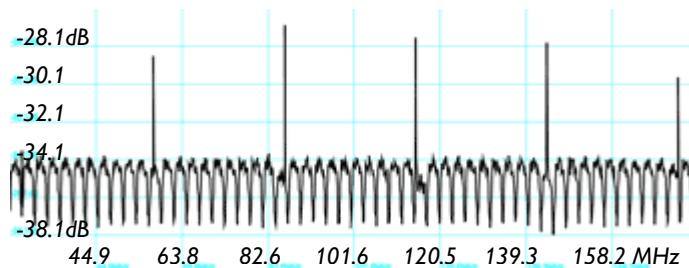

Figure 5. Artifacts from the 28.8MHz local clock oscillator. (Graphs produced by RTL_SDR_Wide_Spectrum_Analyzer.)

These artifacts are a reminder that this hardware was not designed for the purpose of emulating a spec-

trum analyzer. In this 150 MHz-wide segment of spectrum, the maximum resolution is 150 kHz. It takes several seconds to generate this data. A professional instrument would have a higher resolution with much less delay. Lastly, the dongle is prone to artifacts resulting from nonlinear mixing in the front end. For instance, my Kenwood TS-590SG was used to transmit a CW signal into a dummy load. The dongle was positioned nearby with a separate dummy load on the antenna input. When the transmit power was increased to 15W, not only was there a signal present on the transmit frequency of 52 MHz, there were artifacts on 50.9 MHz and 53.1 MHz.

FM radio spectrum

The SDR spectrum analyzer was able to examine signals on a portion of the FM broadcast band. A magmount antenna designed for 2 meter amateur use was connected to the device. As mentioned previously, one would expect oscillator artifacts at 86.4 and 115.2MHz. Frequencies between 89 and 114 MHz are shown in the figure. At my QTH in Yorktown Heights, the strongest signals measured in this range were at 90.7, 100.7, and 106.3. This corresponds respectively to WFUV (Bronx), WHUD (Philipstown), and WFME (Mt. Kisco).
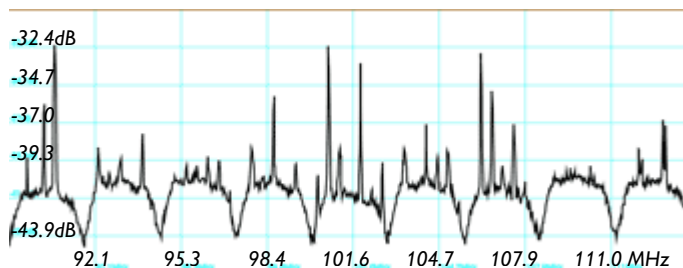
Figure 6. FM Broadcast Stations, 89 - 114 MHz

Filter measurement

The SDR spectrum analyzer can also be used to characterize RF filters. I purchased an inexpensive noise source, marked **BG7TBL**, on eBay for approximately $11.00. I powered the noise source with 6V DC instead of the suggested 12V, as the spectrum analyzer software often crashed at the higher voltage. When the output was connected to the dongle's antenna jack and the signal was measured between 142 to 162 MHz, it generated the results shown in Figure 7.
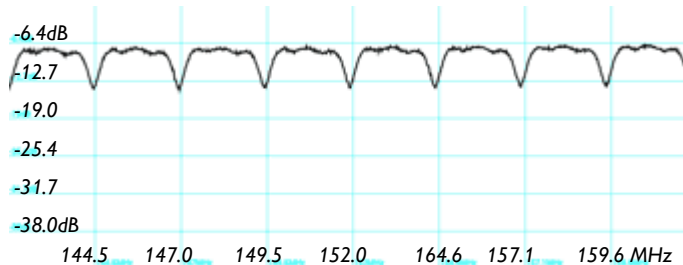
Fig 7. Signal amplitude of noise generator, 142 - 162 MHz.

A commercially-made bandpass filter was then connected between the two devices. Figure 8 shows the signal over the same frequency range. While the stop-band attenuation is significant, a familiar artifact appears at 144 MHz, which is the 5th harmonic of 28.8 MHz. One would not expect an external filter to attenuate a signal generated from within the dongle.
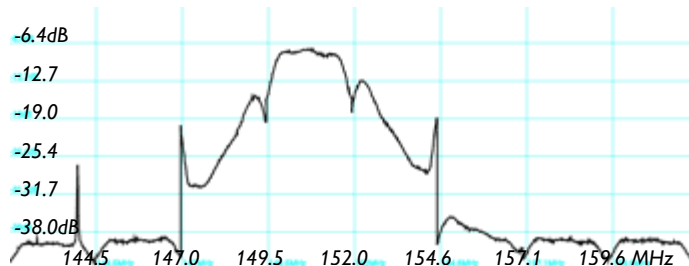

Figure 8. Signal amplitude of noise generator in series with bandpass filter. [Same frequency range as fig. 7.]

Table 1 shows the difference in amplitude at various frequencies. There was less than 1dB attenuation in the passband and over 30dB attenuation in the stopband. I must express my gratitude to Bob N2CBH — not only did he donate the filter to the club auction, he also provided editorial assistance with this newsletter article.

Frequency MHz	Amplitude Fig 8	Amplitude Fig 7	Attenuation dB
146.2	-39.5	-8	31.5
147.5	-30.5	-7.3	23.2
149.2	-15.4	-9.2	6.2
150.0	-7.9	-7.3	0.6
151.5	-8.4	-7.9	0.5
152.3	-12.8	-7.9	4.9
154.0	-27.6	-7.9	19.7
155.0	-35.7	-7.3	28.4
156.0	-38.9	-7.5	31.4

Table 1: Signal attenuation — measured as difference between signal amplitude of noise generator direct and in series with the commercial bandpass filter.

Although I haven't tried it, one can also build an antenna analyzer with this hardware. A directional coupler would be needed for measurement of return loss and VSWR, but the price is minimal. It is clear that today's amateurs have the opportunity to build usable test equipment at low cost. Perhaps in the future, they won't even have to make the effort? Opportunity exists for major manufacturers to build an SDR transceiver according to a new paradigm: a single device that works reliably for amateur communications, but can also perform accurate data measurement, supplanting the need for additional test equipment. These radios will redefine the concept of a "shack-in-a-box."

- Lou, KD2ITZ

Icom Club Net

As announced at the February meeting, Lou KD2ITZ has registered PCARA in a monthly contest organized by Icom America. Their web site explains:

Club Net
Amateur radio is all about community. Icom knows that ham clubs play a big role in bringing hams together to network and learn from one another on an ongoing basis. As a way of giving back, Icom has launched a promotion exclusively for ham clubs! By registering, your ham club could win Icom swag, a Skype presentation, an in-person presentation or an Icom radio! Register today for your chance to win!

Registration with Icom required the radio club name, call sign and address, plus details of club activities including meetings, Field Day, fox hunts and repeaters. PCARA has now been awarded "2019 - Segment 1 Monthly Winner" with the following write-up on Icom's web site:

January
Peekskill/Cortlandt Amateur Radio Association
Peekskill/Cortlandt Amateur Radio Association (PCARA) is a nonprofit organization 501(c)(3) consisting of a dedicated group of volunteers and communications infrastructure accessible in Northern Westchester, Putnam, and beyond. For nearly twenty years, PCARA has been a source of knowledge and camaraderie for individuals throughout the Hudson Valley. Learn more about PCARA at PCARA.org
[https://www.icomamerica.com/en/amateur/club-net/winners.aspx]

Lou reports that the merchandise should arrive in 4-6 weeks. Items in the "club swag kit" are likely to include an Icom 'Ham Crew' T-shirt, water bottle, hat and backpack. There is also the possibility of a presentation by Icom at one of our meetings later in the year.

V.E. Test Session

PCARA's next Volunteer Examiner (V.E.) Test Session takes place on Saturday March 16, 11:00 a.m. at the John C. Hart Memorial Library, 1130 E Main St., Shrub Oak, NY.

The cost for candidates is $15.00 per exam or re-test. Photo-ID is required, plus SSN if unlicensed. All candidates are advised to contact Mike W2IG before the session using e-mail address: w2igg 'at' yahoo.com.

Passing of Speedpass™

In a few months' time, gas station forecourts will become quieter than they are today… that's quiet in the radio sense.

Exxon™ Mobil™ have sent a notice to users of their Speedpass key tags that the tags are being retired. Some gas stations have already begun phasing out key tag functionality and the system will be fully retired by June 30, 2019.

Speedpass tag clipped onto a vehicle key ring.

The Speedpass key tag system was introduced by Mobil in 1997 in the form of a small transponder that could fit onto a key ring, capable of activating gas pumps at participating stations. The system automatically debits the customer's purchase from a predesignated credit card.

How it works

The system employs radio frequency ID (RFID) equipment from Texas Instruments known as "TIRIS" — for **T**exas **I**nstruments **R**egistration and **I**dentification **S**ystems. The equipment is installed in some 10,000 Exxon, Mobil and Esso gas stations worldwide.

A Mobil customer who has registered with Speedpass holds the key tag close to the 'Pegasus' flying horse logo on the

Mobil gas pump with Speedpass Pegasus logo arrowed (left).

gas pump. Once the key tag has been successfully interrogated by the pump, the logo is backlit and the tag's ID is transmitted to a central billing location. After the gasoline has been pumped, the system charges the cost to the customer's pre-registered credit card. The credit card number is not stored in or transmitted by the tag.

A vehicle-mounted version of Speedpass was also available. This took the form of a small transponder (similar to EZ-Pass) mounted inside a vehicle window close to the filler cap.

Speedpass panel.

The original intention was to speed up transactions at the gas pump, at the same time increasing customer loyalty to Mobil. This speed-up was certainly a factor in the early days of Speedpass when the alternative was to pay at the gas station counter with cash or pull a credit card out of the wallet.

Radio-frequencies

Speedpass key tag transponders are passive devices that are powered by the external reader, mounted in the gas pump. The tags operate in the low frequency (LF) range of 30-300 kHz using a frequency of 134.2 kHz. As the tag is placed within a few inches of the 'Pegasus' logo on the gas pump, a magnetic coil antenna behind the bezel sends out a 15 to 50 millisecond pulse of RF energy on 134.2 kHz. The coil antenna is not large enough to radiate an electromagnetic wave efficiently, but the magnetic near field is sufficiently strong to be picked up by the small coil inside the customer's key tag. The LF signal generated by magnetic induction is rectified and charges up a capacitor. Once the transponder is powered up, it can transmit and respond to signals from the gas pump reader.
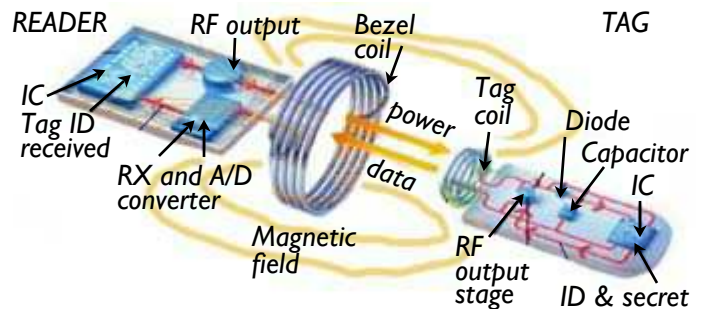

Diagram of low-frequency RFID reader and tag, as used in Mobil Speedpass key tag system.

In order to avoid unauthorized cloning, the key tag's information is partially encrypted. The gas pump reader transmits a binary sequence to the tag as pulse-width amplitude modulation of the 134.2 kHz carrier. The key tag responds by transmitting a signal with frequency shift keying between 134.2 kHz and 123.2 kHz. The challenge-response sequence begins with the pump reader transmitting a 40-bit challenge code. The tag encrypts this challenge using a secret 40-bit key stored in the tag, then returns its own ID code and a 24-bit encoded response. The reader can then verify that the tag's secret key is correct and authorize the credit card transaction. The entire sequence takes only a few milliseconds. Storing a secret key in the tag's electronic circuitry was intended to prevent cloning of the tag by unauthorized interception of the radio frequency signals and responses.

In the original implementation, communication from the gas station to Mobil's credit card data center took place via satellite dish and Hughes Network Systems' satellite hub.

Vehicle mount

Mobil also required a vehicle-mounted transponder as part of its Speedpass system. This transponder is battery-powered, dual-frequency and mounted on a vehicle window near to the fuel filler cap. The transponder is activated by another 134.2 kHz LF signal — though the transmit antenna for the vehicle tag is separate from the bezel coil and takes the form of a wire loop inside a plastic frame high above the gas pump.
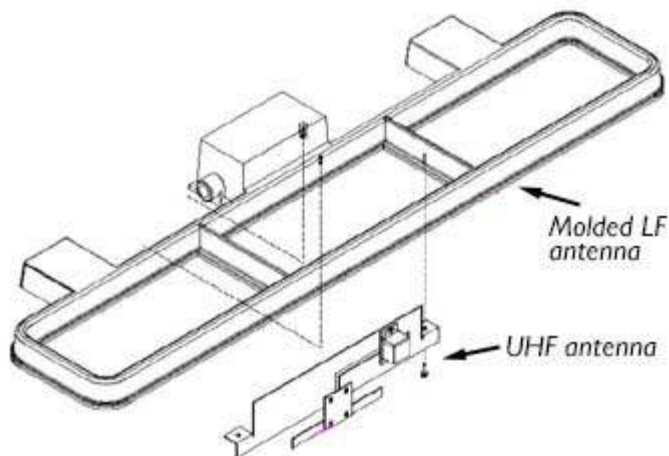

Diagram of original Speedpass antennas for communication with vehicle-mounted transponders, using LF transmit toward and UHF receive from the vehicle.

The response from the vehicle transponder takes place on UHF at a frequency of 902.858 MHz. This signal is picked up by a sheet-metal slot antenna which is positioned above the gas pump, covering an area of a few feet around the front of the pump. At the time of writing, these antennas were still visible at Mobil stations.

Looking up into the top of a Mobil gas pump reveals the molded plastic LF antennas for sending to the vehicle's transponder and slot antennas for UHF reception.

Speedhack

In 2005 the key tag's encryption code was broken by a team from the Computer Science Department at Johns Hopkins University in Baltimore, MD and person-nel from RSA® Laboratories in Bedford MA. The team reverse-engineered the Speedpass challenge-response protocol and recovered the secret key from a tag by monitoring its RF responses. They were then able to purchase gasoline at a gas station using a simulated tag. See the following for details:

https://www.securityevaluators.com/casestudies/exploiting-rfids/

PDF Document: https://www.securityevaluators.com/wp-content/uploads/2017/07/tiris.pdf

Speedpass customers now have to enter their ZIP code using the pump's keypad as an extra layer of security before each gasoline purchase can be authorized.

Why goodbye?

Exxon Mobil have not given any explanation of *why* their Speedpass key tag system is being retired. Breaking of the encryption code might be part of the story, but there could be other reasons. After 22 years, the pump RF equipment and tags are both getting old and would be expensive to replace. Newer vehicles no longer have a physical lock and key to enter the vehicle and start the engine — instead they rely on a wireless fob that might be buried deep in a driver's pocket or bag. And credit cards have themselves grown smarter — chip cards work together with the payment terminal to generate a one-time code, allowing each transaction to be authorized, while making the card more difficult to clone.

Exxon Mobil have recommended that Speedpass key tag customers should download the free "Speedpass+™" app to their Apple or Android smartphone. All the customer has to do at the service station is select the pump number then tap a button on the phone to authorize payment from the car seat before getting out to pump gasoline.

No help is offered to customers without a smartphone!

- NM9J

Signal generator review

Out with the old

When I acquired my new oscilloscope (see *PCARA Update*, February 2019 p 11), one of the first things I did was connect a vintage audio oscillator as a source of sine waves. Unfortunately, the waveform displayed was far from perfect.

My old audio oscillator was home-built in the mid-1970s, while I was living in Southport, NW England. It was based on a Wien Bridge oscillator circuit, with dual variable resistors and switched capacitors to set output frequency in the range of 15 Hz to 150 kHz. I had built the unit myself at a time when commercial test equipment was quite expensive and home construction provided a lower cost alternative.

Home-brew audio signal generator from the mid-1970s. Control knobs are ex-Pye.

To see what might be wrong, I popped the cover off the metal box and saw a circuit built on Veroboard (stripboard) with discrete BC108/BC109 transistors, Mullard multicolored polyester capacitors, powered by a large, heavy 12 volt AC transformer. The aluminum chassis, coated in blue Hammerite metal finish paint and labeled with "Letraset" rub-down dry-transfer letter-

Inside the old audio signal generator.

ing looked as good as new. The 12 volt transformer bolted to the chassis was rated at 240 volt AC input with *no* 120 volt tap. In fact, this was the last item of shack equipment from Britain that still needed a 240 volt AC supply, derived from an external auto-transformer.

Inside the box, I noted that at least one wire had come adrift. I could not remember where the original circuit came from… I checked ARRL *Handbooks* and RSGB *Radio Communication Handbooks* from the period, but could not find a matching schematic. An online search also came up short. Reluctantly I decided to retire the 45 year old unit and seek something more modern for generating audio tones.

In with the new

An online search revealed that modern signal generators have moved on a great deal since the 1970s. Instead of a free-running oscillator dependent on variable resistors, the signal is now generated by **direct digital synthesis** (DDS), just like our modern HF transceivers. I picked out the "Koolertron CJDS66 series" available through a well-known online vendor. Five different models are offered, with maximum sine-wave frequencies of 15, 30, 40, 50 or 60 MHz. I ordered the 60 MHz model, which arrived a few days later as it is stocked in the USA. It turned out to be a re-badged version of the **Junce Instruments JDS6600** series. These units have a price between $80.00 and $140.00, depending on the maximum frequency specification and the vendor.

Out of the box

Inside the shipping container was the signal generator itself, an external wall-wart power supply rated at 5 volt 2.0 amp, a BNC to BNC cable, two BNC to alligator clip cables, a USB A-B cable and a small format CD-ROM disk. There was also a slim, printed "Operating Manual" of 12 pages.

Items shipped with the DDS Signal Generator include a slim manual, USB cable, BNC cables, mini-CD-ROM and 5V PSU.

The signal generator is housed in a beige plastic box with tilt bail to angle the front panel upward. The box weighs next to nothing (2 lb according to the spec), something you immediately notice when trying to connect a BNC cable with one hand… the unit goes sliding across the test bench! Size of the enclosure is 8" wide by 3½" tall by 7½" deep.

Switching on power using the front panel on/off button gives a brief "Loading…" screen which identifies the unit as a "DDS Dual Channel JDS6600-60M, Signal Generator/Counter, P/N: 1726600000. There is a one-time request to choose language, then the main screen appears. Subsequent pressing of the SYS button on the front panel brings up a "System Setup" screen with model number and part number, followed by a link to http://www.junteks.com, the web site of Hangzhou Junce Instruments Co., Ltd. of Hangzhou in East China. This confirms the Koolertron ⇆ Junce "badge engineering".

Bright lights

The front panel has a brightly lit 2.4" liquid crystal display (LCD), with five "soft keys" arranged down the right side of the color screen. The front panel has nine more push buttons, a rotary control and three BNC sockets labeled "Ext. IN", "CH1" and "CH2".
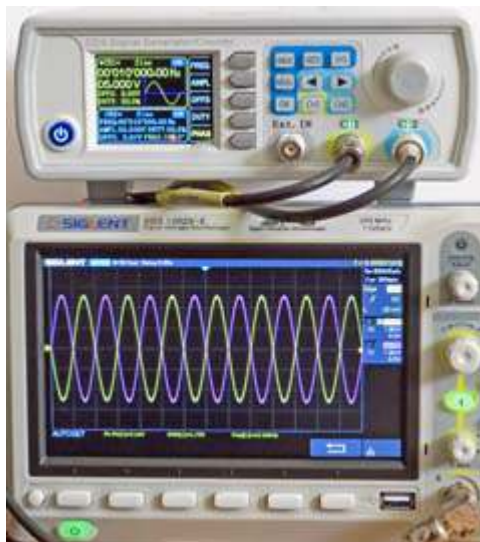

Front panel of the Junce JDS6600 DDS Signal Generator.

After power-up, the color display is split into two parts, with the upper section in yellow dedicated to "CH1" the Channel 1 BNC output. Default settings are sine wave output, a frequency of 00,010,000.00 Hz (10 kHz) and an amplitude of 05.000V (peak to peak). The lower section of the display in blue is dedicated to "CH2" the channel 2 output. Both channels are "on" at power-up, as indicated by green LEDs.

Connecting channel 1 and channel 2 to my oscilloscope with BNC cables confirmed that 10 kHz sine waves were present, though peak-to-peak voltage was a little more than 5 volts. I also discovered that the BNC cables supplied with the signal generator were unreliable – wiggling the cable's BNC connector at the instrument caused an intermittent connection. This was fixed by substituting a pair of quality 50 ohm BNC-to-BNC cables previously purchased at a local hamfest.

Sine wave outputs from Channel 1 and Channel 2 displayed on Siglent scope.

Maximum output from the signal generator is specified as 20V peak-to-peak up to 10 MHz, 10V from 10 to 30 MHz and 5V from 30 to 60 MHz. Sine waves are available up to 60 MHz, but the more complex waveforms are only specified to 15 MHz (square and triangle) or to 6 MHz (Pulse, CMOS, Arb).

Knobs and buttons

It takes a few minutes to get used to the instrument's front panel controls. Nine buttons have dedicated functions — for example WAVE allows access to the main screen for adjusting frequency and amplitude, while MOD allows access to a

Signal generator has nine buttons with fixed functions and one rotary control.

separate screen for setting modulation types such as frequency sweeps. The MEAS button changes mode from signal generator to frequency counter/period measurement.
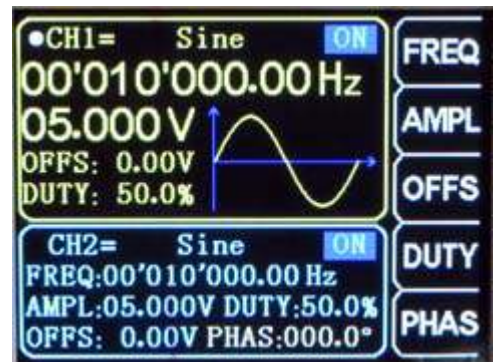

WAVE screen for adjusting frequency and amplitude of CH1 and CH2 output signals.

There are two dedicated buttons labeled '◄' and '►'. They can be used for horizontal navigation along a line of digits when adjusting either frequency or output voltage.

The other front panel control is a rotary selector knob, which has 24 click stops per revolution. This control can be used to increase or decrease the digits of a frequency or voltage… and for selecting other items in the menu system.

Wave goodbye

Pressing the WAVE button a second time moves the screen highlight to "Sine" at the top of the screen, and changes the soft keys to depictions of
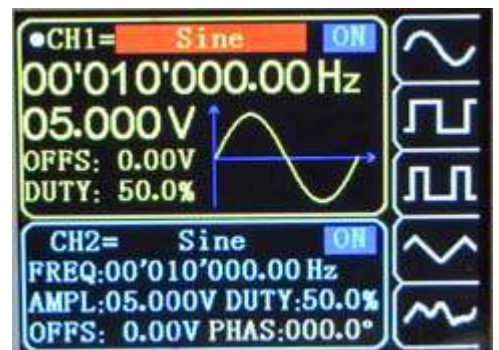

"Wave" selection.

sine, square and triangle waves. Eighteen waveform choices are available by turning the rotary control including: Sine, Square, Pulse, Triangle, Half wave,

Ladder, Noise etc. At the end of the pre-programmed choices are "Arbitrary01" to "Arbitrary15" — these are waveforms defined by the user and stored in generator memory. See the subsequent section for more details.

Modulate

Pressing the MOD button brings up the 'Modulation Mode' screen. There are four choices available. "S. F (CH1)" is swept frequency mode, with the default

output being the current waveform, swept in frequency from 1 to 10 kHz. Start and end frequencies, sweep time and direction can all be programmed from the front
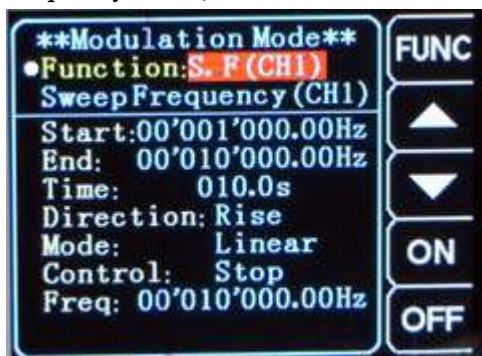
Signal generator's 'Modulation Mode' screen allows access to swept frequencies.

panel. I set a range of 14.000 MHz to 14.010 MHz then monitored the result on my HF transceiver set to the 20 meter band.

This type of swept frequency operation could be valuable for plotting the response of audio frequency or radio frequency filters.

The other modulation modes are 'S. F (CH2)' — swept frequency for channel 2, "PLS (CH1)", which is a pulse generator with pulse width and pulse time (in nanoseconds) adjustable from the front panel and "Burst (CH1)" which can generate a train of pulses, triggered by CH2 or an external trigger.

For radio purposes, there are some obvious missing features — there are **no** choices available in the menu system for amplitude modulation, frequency modulation, frequency shift keying or external modulation. There may be a workaround — see the following sections.

Remote control software

Remote control software for the JDS6600 is supposedly provided on the mini CD-ROM. Online videos by "Rd Tech" describe how to install the software on a Windows computer for remote control of the signal generator and how to use the software to define an arbitrary waveform. (Search for JDS6600 on YouTube).

I began my software installation by examining the supplied mini CD-ROM. It contained a single file "DDS Signal generator.rar". Unfortunately, when I tried to expand this file using WinZIP the message was "not a valid RAR file." On the AliExpress page (https://www.aliexpress.com) for the RD JDS6600 I found a link to the desired software which is available on

mediafire.com. I downloaded the file "JDS6600 CD file 11.17-1.zip" to my Windows 7 notebook then expanded it using WinZIP. Always suspicious of anything free from the Internet, I gave the result a couple of scans with Anti-virus software — all was well.

Installation instructions provided on the (silent) YouTube video are to run the expanded program file JDS6600.exe — this brings you to the Main Menu where you should first choose a language (English) then work through the steps: 1. Install USB Driver, 2. Install NI-Visa, 3. English Main Program, 4. View Manual. When this was completed, I restarted the computer, plugged in the A-B USB cable from the JDS6600 signal generator and switched on.

A window appeared announcing that the driver software was being installed. I also noted that a new icon had been added to the desktop, labeled JDS6600.

Software capabilities

Running the newly installed JDS6600 software brought me to the "JDS Signal Generator" screen, at the "Configuration" Tab. This allows the USB serial port to be specified… in my case it was COM12. Clicking "Connect" filled out the model and serial number automatically. Three additional tabs are available: "Control Panel", "Extend Function" and "Arbitrary".

The Control Panel tab duplicates the capabilities of the signal generator's front panel. You can set frequency, amplitude, waveform, phase etc. for both the CH1 and CH2 outputs.
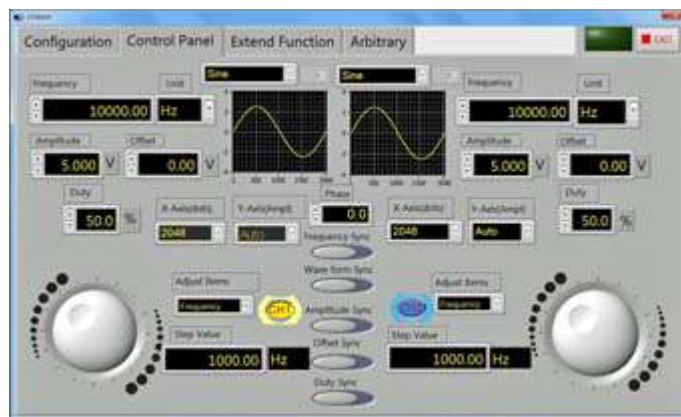
'Control Panel' tab of the JDS6600 software simulates the front panel controls for CH1 and CH2 outputs.

The "Extend Function" tab allows measurement of frequency and period. It also duplicates the facilities of the Modulation Mode screen for frequency sweeping and pulse generation.

The "Arbitrary" tab is the place to define and store arbitrary waveforms in the signal generator's memory. Unfortunately, there are no written instructions for this procedure — all I had to go on was the brief video by "RD Tech" on YouTube. There isn't room to go into details here, but you are provided with capabilities to define up to 2048 points for one cycle of a repeating

waveform — either by drawing the points in an on-screen graph or by importing one of the predefined waveforms, e.g. sine, square, triangle etc.

After a few tries, I was able to 'draw' an amplitude-modulated waveform as the product of two sine waves using the formula:

$$E = E_0 (1 + m.\sin 2\pi f_m.t) \sin 2\pi f_c.t$$

…where f_c is the carrier frequency and f_m is the modulating frequency. I used a carrier wave with a frequency roughly 100 times the modulating frequency so I could fit ~100 cycles of carrier within the 2048 points allocated to one cycle of the lower-frequency modulating waveform.
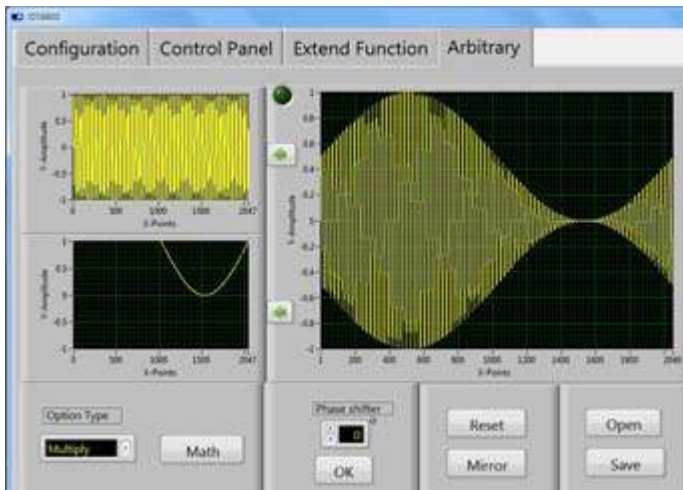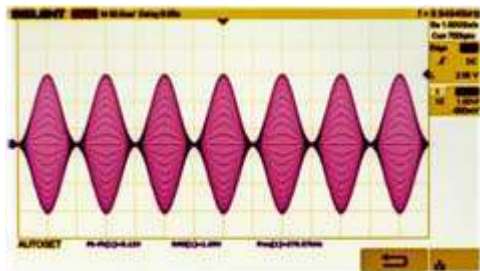

Partial screen-shot of "Arbitrary" tab in JDS6600 software, showing simulation of an amplitude-modulated sine wave.

After the mathematical operations on the computer's screen were satisfactory, I stored the resulting waveform in the signal generator's 'Arbitrary01' user-defined function and was pleased to see the effect reproduced on the oscilloscope connected to the signal generator's CH1 output.

Signal generator screen for user-defined Arbitrary01 wave.

The arbitrary waveform stays in signal generator memory, surviving power on/off cycles. You can adjust frequency and amplitude just like any other waveform, but bear in mind that the ratio of carrier fre-

Amplitude modulated waveform generated by JDS6600 displayed on Siglent scope. (Colors inverted for clarity.)

quency to modulation frequency is still maintained when the frequency is shifted.

It may be possible to 'draw' other forms of modulation such as Morse code, FM or FSK in a similar manner — but I'm not sure that it's worth the trouble. If you need a radio frequency signal generator capable of the different modes of modulation commonly used in amateur radio, then it might be better to look for a model designed for that task — such as the Siglent SDG1032X — rather than an audio frequency generator with high frequency aspirations.

Conclusions

The Junce Instruments JDS6600 is an inexpensive signal generator for both audio frequency and radio frequency work. Direct digital synthesis gives a number of advantages compared with old analog generators of the past — not least of which is the ability to set an exact carrier frequency. However, this signal generator may not be very suitable for receiver alignment as the plastic case is not shielded and there is considerable noise on the output at the lowest adjustable level of one millivolt. There is even

*JDS6600 signal generator with top cover removed. The plastic case is **not** shielded.*

more noise when a USB connection to a computer is in use. An external attenuator might be needed for very low-level signals. Lack of any radio modulation modes is another drawback. For critical measurements, be sure to substitute some high-quality 50 ohm shielded test cables to replace the inferior variety that accompany the unit as shipped.

Inclusion of a frequency counter covering 1 Hz to 100 MHz is an advantage, though the built-in quartz crystal standard has no adjustment for precise frequency, and it was subject to a warm-up drift of roughly 4 ppm when tested over a period of 30 minutes.

Ability to control the signal generator from a PC and to design arbitrary waveforms is a plus point — though the lack of *any* written documentation for the remote control software slows down the learning process. Investigation of additional hobbyist applications such as testing audio amplifiers and measuring filter response could be worthwhile.

- NM9J

Peekskill / Cortlandt Amateur Radio Association

PCARA Information

PCARA is a **Non-Profit Community Service Organization**. PCARA meetings take place the first Sunday of each month* at 3:00 p.m. in Dining Room B of NewYork-Presbyterian/Hudson Valley Hospital, Rt. 202, Cortlandt Manor, NY 10567. Drive round behind the main hospital building and enter from the rear (look for the oxygen tanks). Talk-in is available on the 146.67 repeater. *Apart from holidays and July/August break.

PCARA Repeaters

W2NYW: 146.67 MHz -0.6, PL 156.7Hz
KB2CQE: 449.925MHz -5.0, PL 179.9Hz
N2CBH: 448.725MHz -5.0, PL 107.2Hz

PCARA Calendar

Sun Mar 3: PCARA meeting, NewYork-Presbyterian / Hudson Valley Hospital, 3:00 p.m.
Sat Mar 16: PCARA Breakfast, Turco's, Yorktown Hgts. 9:00 a.m.
Sat Mar 16: PCARA VE Test Session, John C. Hart Memorial Library, Shrub Oak, 11:00 a.m.

Hamfests

Sun Mar 3: BARA Spring Auction, Westwood Regional HS, 701 Ridgewood Rd, Township of Washington, NJ. 12 noon/1:00 p.m.
Sat Mar 9: Cherryville RA Hamfest, North Hunterdon HS, 1445 Route 31, Clinton, NJ. 8:00 a.m.
Sat Mar 16: New Jersey Antique RC Spring Swap Meet, Parsippany PAL Building, 33 Baldwin Road, Parsippany NJ. 8:00 a.m.
Sun Mar 24: Southington ARA Hamfest, Southington High School 720 Pleasant Street, Southington, CT. 8:00 a.m.

VE Test Sessions

Mar 10: Yonkers ARC, Yonkers OEM, 789 Saw Mill River Rd, Yonkers NY. 11:30 a.m. Pre-reg. John WB2AUL, (914) 969-6548.
Mar 14: WECA, Westchester Co Fire Trg Center, 4 Dana Rd., Valhalla, NY. 7:00 p.m. S. Rothman, (914) 949-1463.
Mar 15: Orange County ARC, Munger Cottage, 183 Main Street, Cornwall NY. 6:00 p.m. Contact J. DeLorenzo (845) 534-3146.
Mar 16: Peekskill/Cortlandt ARA, John C. Hart Memorial Library, 1130 E. Main St., Shrub Oak, NY. 11:00 a.m. Contact Michael Dvorozniak W2IG, (914) 488-9196.
Mar 18: Columbia Univ ARC, 531 Studebaker Bldg, 622 W 132nd St, New York. 6:30 pm, Alan Crosswell (212) 854-3754.

Peekskill / Cortlandt Amateur Radio Association Inc.
PO Box 146
Crompond, NY 10517