The Local Oscillator

The Newsletter of Crawford Broadcasting Company Corporate Engineering

JUNE 2012 • VOLUME 22 • ISSUE 6 • W.C. ALEXANDER, CPBE, AMD, DRB EDITOR

Progress!

May was a landmark month in the KBRT site move project. On Tuesday, May 22, dirt was moving at the site.

The dirt being moved was actually part of the utility trenching project taking place near the NOAA Doppler radar site ¾ mile southwest of the site, the first step to getting electrical power to our property. Over the next two months, the contractor will dig 4,300 feet of 24-inch wide trench with a backhoe and lay in conduit, installing concrete pull-boxes every few hundred feet. Once this trenching gets to our property, a concrete pad will be poured for the Edison transformer that will step the 12 kV primary power down to the 480 volts that we will need for the KBRT transmitter site.

Quite the crowd up at the new KBRT transmitter site at Oak Flat

I was at the site on the 22nd, and it was a beehive of activity with all kinds of construction equipment operating. Two of the workers opted to live in a travel trailer on our property, saving them the 20-minute drive on the switchback dirt road twice a day. This also serves to provide security for the contractor's equipment, tools and property.

Also on that date, we held a meeting with the folks from P&R Tower (Magnum), their drilling, concrete and pumping subcontractors, our project engineer, civil engineer, Bill Agresta and Todd Stickler at KBRT. In this meeting, we went over all aspects of the project and developed a project timeline that was then distributed to the bidders at the pre-bid meeting and site walk-through later that day. We fleshed out many of the details that had to that point been just concepts.

At the time of this writing, we are in the middle of the bid process for all parts of the project other than towers. We hope to award a contract shortly, pull the permits in early June and get started with the grading by the middle of the month. Once grading is done, the tower work can commence, and that will take about six weeks to wrap up. Then after the towers are up, we can move on to the other parts of the project – transmitter building, security walls, etc. We could do some of that sooner, but it would be costly. It is much better and less expensive to consolidate all the pier drilling, the foundation work, concrete and other trades than to bring each trade back several times for small parts of the project.

The project is still on track for completion late this fall.

Burnout

Last month, the WMUZ main transmitter began tripping off with high VSWR. This happened in good weather and was apparently unrelated to lightning or any environmental factor.

Chief engineer Joe Huk was able to patch the main transmitter into the auxiliary antenna, which is identical in every respect except elevation to the main antenna, and get the station on the air at full power.

A few days later, we were able to get Great Lakes Tower to climb and locate the issue. They

started with a TDR shot of the line, which revealed an anomaly some 60 feet below the antenna. A climb quickly revealed an externally visible burn right at that level. The tower was rigged and several line sections were removed. The problem was apparent: a classic "burned bullet."

The burn location was clearly visible on the outside of the line section.

For the uninitiated, a "bullet" is the plated connector that joins through spring tension the inner-conductors of adjacent line sections. Normally, the bullet has a large area of contact, and the spring tension keeps the fingers of the bullet pressing tightly against the copper of the inner-conductor tubing. A Teflon disk is typically installed on the bullet, right in the middle to keep the bullet and adjacent inner-conductors centered within the outer-conductor.

What occasionally happens is that a small impurity gets between the plated bullet fingers and the copper of the inner-conductor. This probably happens during installation. That impurity or contaminant can be there for many years without issue, but eventually it produces a little bit of oxidation of the copper or bullet plating. That little bit of oxidation exhibits some electrical resistance, and the RF current flowing through that little bit of resistance produces heat. That heat produces more oxidation, which produces more resistance, which produces yet more heat – the classic thermal runaway. Eventually, things start to melt, and at some point there is enough of a discontinuity to get the transmitter's attention, or else an arc occurs, usually across the Teflon disk (where residue from the burn accumulates and creates a carbon path).

Thankfully, we have a storage building full of the exact same type of Dielectric 3-1/8 inch rigid transmission line in Chicago. The tower crew was able to drive over and pick up the pieces they needed to replace. The adjacent pieces were thoroughly cleaned, and the main transmission line and antenna were quickly returned to service.

Other than taking great care to prevent contamination during installation (such as keeping fingers off the inner-conductor and the metal part of the bullets) and maintaining good pressure with nitrogen or dry air, there really isn't much you can do to prevent this kind of thing. You could periodically take the line down and clean it, but that invites all kinds of other issues. You could do a periodic TDR sweep of the line, but in my experience the time is very short, perhaps hours, between a problem first appearing and a catastrophic meltdown. Unless you were lucky enough to sweep the line right before the

A classic "burned bullet."

thermal runaway occurred, you probably wouldn't see it anyway. There are some folks out there that use infrared imaging to detect "warm" bullets, and that may provide the best external indicator of a developing problem.

The best course of action is to make sure your transmitter's VSWR detector is properly adjusted, or to employ an external "Wattcher" that is tied into the transmitter's interlock circuit. By the time the transmitter or Wattcher detects the problem, the bullet will already be burned, but you may be able to salvage the adjacent pieces of line.

The New York Minutes
By
Brian Cunningham, CBRE
Chief Engineer, CBC – Western New York

Hello to all from Western New York! In last month's report, I brought up the subject of security within our station walls and situations in which an employee might commit theft or sabotage against the station. This month, I'll continue along those lines by discussing what you can do to lessen the chances that your station property can be stolen, sabotaged or tampered with. After all, as engineers we are charged with the responsibility of protecting our stations' assets on every level, not just maintaining the facilities and equipment. Those assets can be either tangible or intangible. Tangible assets are those things that someone can physically remove from your station for personal use or to sell for money. Intangible theft could be electronically diverting funds from one account to another, theft of intellectual property and even identity theft.

What happens when you suspect or catch an employee committing theft in your station? Most people's first thoughts are, is it legal or can I be sued for investigating privately a suspected thief? Two well-quoted areas of legislation which are often perceived as a standard to investigating are "The Human Rights Act" and "RIPA – The Regulatory Investigation of Persons at Work Act." In many well documented cases in the past, when an employee is caught stealing from his/her employer, they try and use these legislations in their defense, but if all of the policies and procedures are followed within both acts, this legislation actually assists the person investigating the crime and protects the station against wrongful lawsuits. This legislation is too large and in depth to discuss here, but it would be worth your while to read up on these topics, if and when you suspect an employee of theft.

Implement anti-theft measures

Keeping your station safe and secure is not an easy task. In many of today's radio markets, the engineering staff is expected to do more with less manpower, so how do you go about protecting your company's assets? First and foremost, keep an accurate inventory of your assets. If you don't have an in-depth list of all your equipment and its location, it's very easy for several items to "disappear" without being noticed. This is especially true for equipment that has been taken out of service and is not used on a regular basis. This would include all equipment that has been retired because of age, pulled from service to repair or not used regularly, such as remote broadcast equipment. Inventory each and every item that has a value of at least $100. Attach an inventory asset tag at a convenient location on the front of the unit, so when inventory time comes, it can be identified quickly and efficiently. To help prevent thefts, occasionally perform random inventory spot checks. This will let potential thieves know that the equipment has been inventoried and would be missed if taken. All equipment taken out of service should be stored in a secure (locked) environment, and again, spot checked at random times to insure that none has "walked off."

Any company-owned equipment that is not being used, e.g. cassette decks, etc., should be removed and securely stored. Look around your studios and production facilities for any small items that could easily be pocketed, such as mini digital recorders, microphones, and accessories. Make sure that they are clearly labeled and tagged as station property. Keeping a list of these items will aide you in keeping track of the smaller items not included in the main inventory.

Protecting Against Malice or Sabotage

There are many ways in which an employee can commit malice or sabotage against your station. Often times, the person committing sabotage is a disgruntled employee who feels that sabotage is a good way to get back at their employer for inadequate compensation, unequal treatment, or

working conditions that the employee feels are unfair. Most feel that what they are doing is not really a crime, as they have not actually removed property from the station or financially gained from their actions. Generally, these acts of sabotage against the company are computer related, and the perpetrator had unsecured access to important areas of computer files or configuration databases. If your office computers are not protected against intruders, realistically, monies can be transferred to personal accounts and ledgers doctored to cover up any discrepancies. It is a good idea to have more than one person entering data into the stations' books. Engage two or more people in the process of recording and processing stations financial transactions, and never use a signature stamp for signing checks. These have become so commonplace that banks never suspect that a stamped signature could be fraudulent.

On the broadcast end, secure the configuration section of the NexGen computers, with only one or two persons having access to the configuration menus. By having the config menu open and unprotected, anyone could get in and delete specific events, files, and programs in the station log. Remember, your music and commercial spots in the automation system should be considered "inventory" and protected as such. Give your employees only enough rights in NexGen to properly do their job. Leaving this area open and unsecured leaves you vulnerable and provides the opportunity for a disgruntled employee to make your life miserable.

Along the computer lines, never give full rights to the person using the laptop or desktop computer assigned to them. Any configuration or changes to the operating system should be performed by the chief engineer or the person designated to handle IT at your station. Each workstation should be assigned a username and password, for the employee to gain access to the computer, and there should be an administrator password to gain access to the computer, should the employee be let go. Never give out your login credentials to other employees, no matter how much you trust them. It could potentially cause you problems in the future.

Most importantly, any computers that need to be accessed from the outside world have to be secured from unwanted access. Make sure that you have an active firewall and that the security password is unique and could not be figured out easily. WXYZ-01 is not a secure password, and could probably be figured out in a matter of minutes by professional hackers. Again, any VNC access should only be given to those who have a *need* to get into specific networked computers, and the passwords should be changed periodically. It is a good idea to include upper & lower case letters along with numbers when creating the unique password. It is a good idea to designate one person on your staff who would keep a master list of all usernames/passwords of all the stations computers. Generally, this would be the office manager or someone who only has locked access to the stations business records or important documents.

There are many other ways to protect your station from inside thefts and vandalism, and it would take up way too much space here to go through all of them. The most effective measure of station security that many already have in place is video surveillance. Persons are less likely to commit a crime if they know that video cameras are strategically placed within the perimeter of the station. It would be impossible to argue against a videotape showing you leaving the front door of the station with a CD player under your arm.

In order to prevent or detect employee theft, I would recommend implementing the following practices:

- Set a high moral and ethical standard at the top, and insure that standard is communicated down through every level of the organization. Management must model and reinforce that standard.
- Enforce a zero-tolerance policy for employee theft/fraud of any sort, and specifically include in this policy exactly what constitutes stealing.
- Screen all job applicants thoroughly, and conduct background checks on those persons hired in a position of trust
- Implement an anonymous tip-line for employees to report any illegal or immoral activities noticed by co-workers while at the workplace.
- Maintain a positive work environment and be as consistent and fair as possible. Invite open communication with all your employees, especially those who work part-time, which is mostly at night and on weekends. This group, it has been found, is most likely to commit theft or crimes against their employer as they feel that they are unappreciated and underpaid. These feelings usually evolve from a lack of communication and acknowledgement from management. The hardly ever hear from anyone other than their immediate supervisor, and to be acknowledged for doing a good job or complimented for any

other action would go a long way in keeping the communication lines open between upper management and part-time employees.

WDCX-FM – Buffalo, WDCX(AM) / WLGZ-FM – Rochester

Last month, while checking the occupied bandwidth measurements for WDCX(AM), I found the spectrum to be quite high on both the digital sidebands and the intermod readings. I employed the help of Nautel to try and get the levels back down to within the NRSC mask. With tech support assisting via telephone, we checked several readings and made changes within the software to bring the levels down. but regardless of what level we changed, no change was noticed on the spectrum analyzer. Thinking that something had frozen in the software, I was instructed to reboot both the Exporter and IBOC Exciter. When they came back up, the exporter could not communicate with the exciter. Knowing that the units would have to go back to Nautel for service, I switched exciters and brought the transmitter up in analog only.

It has been several weeks since the units have been shipped out, but as of this writing I have not heard from Nautel as to what was causing the problem. Hopefully, by next month I will be able to report on the findings and solution to this problem.

Operations at WDCX-FM and WLGZ-FM have been running rather smoothly thus far, with no major incidents to report on. We have had the usual air conditioning service calls which occur each spring when the hot weather comes sooner than expected. In almost all cases, the condensing coils have plugged up and need to be power washed to get the air fins unclogged with debris and dirt. At both sites, we do not have water service; therefore we cannot perform the power washing ourselves. It takes over 100 gallons of water and cleaner to effectively clean the coils, so we must contract with professionals who have the equipment to properly get the job done.

That about wraps up another month here in the great northeast, and until we meet again here in the pages of *The Local Oscillator*, be well, and happy engineering!

The Motown Update

By
Joseph M. Huk, Jr.,
P.E., CPBE, CBNT
Chief Engineer, CBC–Detroit

Last month, I had a chance to attend the International Dayton Hamvention in Dayton, Ohio. This is the three- day amateur radio convention and flea market. While attending the convention, one product caught my eye. This product is the C. Crane "CCWiFi" Internet radio. This, in my opinion, was a show stopper.

When we think of listening to an Internet stream, we gravitate to our personal computers and launch our favorite media player like the Real Audio Player, Windows Media Player, Silverlight, iTunes or some custom application and listen to our stream. With this toolkit of players, we can cover the majority of codecs like MP3, AAC, WMA, RA, and OGG. With the form factor of the PC, we naturally think of using a computer to listen to Internet radio streams. To the computer generation this seems commonplace. Traditionally, when we think of radio broadcast, we interface with a stand-alone device that tunes our station in and provides us with ability of performing the human interface more directly. I believe that is where the stand-alone Internet radio provides this traditional interface with the advent of the modern day broadcast Internet stream.

The CCWiFi allows the user to program his favorite streams and recall them by way of 99 presets. In addition, the "receiver" also allows reception of programming by various program providers such as Pandora, Aupeo, and Live365. The device uses the Reciva Internet radio technology standard. In the search mode, you can find most of your favorite stations. If a station is not listed, you proceed to the Reciva web site and provide them with the station you would like to receive. You have the option of leaving them an email or providing them with the link or URL to stream. Subsequently, they make your station request a permanent part of their database. That way, going forward, any future listener would be able to access the station you entered. I have gone through the process of adding stations to their database. Once they test the stream, the station is then active on the CCWiFi radio. This process usually takes about a day.

The audio quality of the radio is excellent. I am surprised how good it sounds with the small enclosed speaker. Station selection and radio control is available through the front panel and remote control. I find that control through the remote is more intuitive. The radio is linked via WiFi or you can connect it directly to your LAN via Ethernet. Not only can this radio play Internet streams but it can play your favorite sound files from your network drives.

The only issue that I have found with the CCWiFi is that there are various stations or streams in their library that indicate you are connecting to them but they never connect. Then the radio retries the connection in an endless loop. In an experiment,

Display shows station tuned and song title and artist metadata.

I entered our flagship station WMUZ-FM in the Reciva database. The station played fine for about a week. Then I found myself trying to connect with no success. I was able to listen to our stream using a PC, but not the CCWiFi. Then, as a test, I rebooted our stream encoder. To my surprise, the CCWiFi tuned in WMUZ like a champ. This indicates that just because the PC is able to tune to the station, it does not mean that you might have another issue with your streaming encoder. This peculiarity will take some further investigation to sort out. Hopefully, by the next edition I will have an answer for you.

Until next time, be safe, and if all goes well, we will be reporting to you from the pages of *The Local Oscillator* next month. Best regards.

News From The South

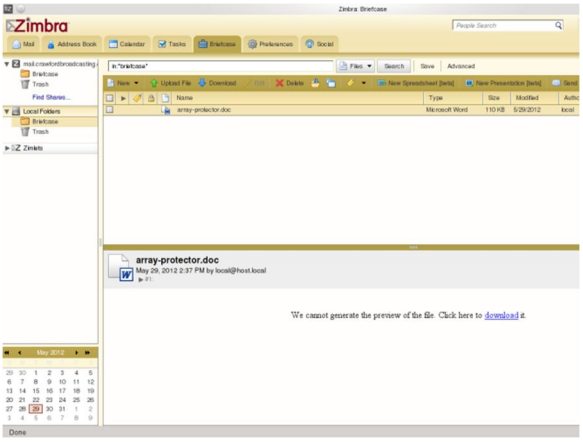
By
Stephen Poole, CBRE, CBNT, AMD
Chief Engineer, CBC–Alabama

Zimbra, Two Months Later

The new mail server is a joy, both to use and to maintain. I have the Zimbra Desktop here at work and I've been trying out some of its more advanced features. Look for some "tip and trick" bulletins from Todd Dixon and me in the next few weeks, as we introduce our users to some of these.

Here's a sneak preview: in either Webmail or the Zimbra Desktop program, you'll see a tab entitled "Briefcase." You can upload files into that, then access them anywhere you have an Internet connection. You may also grant specific users permission to see your briefcase; they can then fetch a file at their convenience. If they accidentally delete it, they won't have to ask, "Could you please resend? Sorry!" They'll simply go back into your briefcase and download a second time.

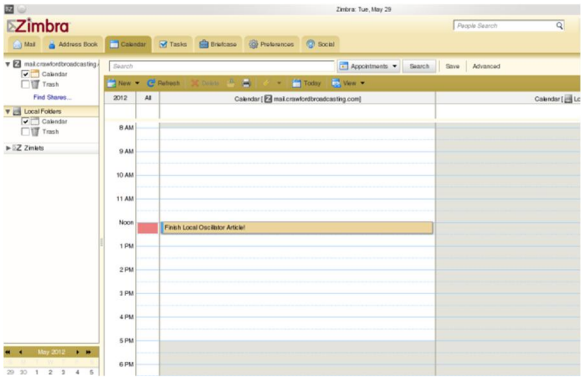
Todd is updating the cheat sheet he sent out on the Briefcase back when we were beta-testing Zimbra; watch for it. At present, we have limited storage on the server, but we're going to expand that as well, to make better use of features like these.



The Briefcase In Zimbra Desktop

One Outlook/Exchange-type feature is the built in calendar. The other day, I was sending an email and said that I would be doing something "next Wednesday." Zimbra Desktop was smart enough to figure out the date (May 30th) and highlight it, in case I wanted to add an event to my calendar. Like the Briefcase, you can share calendar events with selected users. It's an ideal way for small groups to keep up with one another's activities and assignments.

From a maintenance standpoint, Zimbra is a joy, too. With the old Scalix server, I had to knock it down every Sunday evening for at least an hour to make a copy of the entire mail database. I always kept two copies of the database, two weeks' worth of data. Zimbra is so much more reliable and efficient, I can get away with incremental backups: simply put, I only need to copy the *changes* to the backup. It takes about 10 minutes, tops.



A Reminder To Finish This Article!

Thoughts For The Future

Technology keeps changing and we have to keep up with it. You already know that and don't

need me to tell you that. But I've been pondering lately just what instant, world-wide communications means for us – and for the future.

The new wireless technologies and the Internet are by far the most significant communications tools ever. The telegraph and wired telephone, and then radio, television and satellite communications, all had a major impact; no doubt about it. But for the first time in history, Average Joe can now stay in contact with like-minded people worldwide.

(Do you believe that the Earth is flat? There are people who will agree with you online. Join a Yahoo group and complain to kindred spirits that everyone else is brainwashed! It's fun.)

I include smart phones in this mix. Everything from the flash mobs at the shopping malls to the revolutions overseas are powered by instant communications. You email or use a social network to connect with the members of your group, then simply send out a text when it's time to move. Law enforcement (not to mention the odd Middle Eastern dictator) has been caught off guard by this. They're trying to stay ahead of this, but they can't stop it. All they can do is react. And here's the key point:

You *Can't* Censor the Internet

Oh, you can block or censor a single entry point, as we do with our ClearOS firewall coming into the studios and offices. China can, at least to a very limited extent, because they built their Internet from the ground up with limited nodes and careful controls. But the Web at large? Not feasible. Let me explain.

Our Internet here in the United States truly is a "web." If I try to connect to New York and can't make it through Atlanta, I'm automagically routed through Nashville or Charlotte instead. Our local ISP, Hiwaay, for example, actually has a triangular backbone arrangement: from Atlanta to Birmingham, Atlanta to Huntsville, and then between Birmingham and Huntsville. If any one pipe goes down, the most I'll notice is a bit of a slowdown. The larger ISPs have even more redundancy and routing options.

When you hear politicians speak of "controlling" the Internet, or censoring certain Websites, that's a lot more difficult than most people even realize. Some pundits claim that these politicritters are just trying to impress their base supporters, but the truth is even worse: *they don't have a clue*. As far as they're concerned, if AT&T can block or tap a phone connection, your local ISP should be able to prevent you from going to an "unapproved" site. But the only way this could work would be for each ISP, nationwide, to institute filters on each and every connection. That would not only be disruptive, it would cost a megaton of money. Not likely to happen.

Another approach is to shut down Websites that break the law. As I related last time, though, the problem is that these crooks will simply move to a new domain the next day. If you keep shutting them down in the United States, they'll eventually move to a server overseas, outside of US jurisdiction.

For better or for worse, we're stuck with what we have. Good sites and bad are out there on the Internet, so it's up to us to ensure that the company's bandwidth is used properly. You can (and should) use some form of filtering, such as the ClearOS content filter and firewall. Yes, it slows your Internet access and yes, it makes mistakes: sometimes bad stuff gets through and sometimes legitimate sites are blocked. (The best one I've seen yet is when it blocked a page of plumbing supplies at Lowes, telling me that the "weighted phrase limit had been exceeded." I don't *even* want to ponder on that one.)

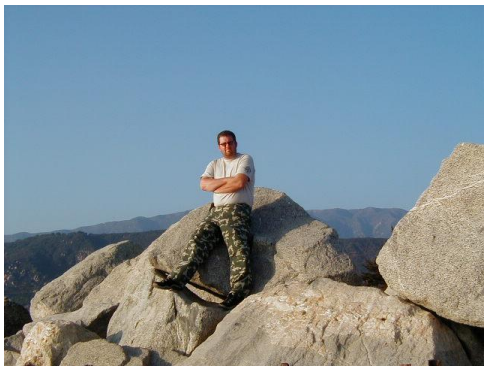
That's about it for this time. 2012 is almost halfway done; let's make the 2nd half even better than the first. Until next time, keep praying for this nation!

Catalina Tales

By
Bill Agresta
Chief Engineer, KBRT

Greetings from Santa Catalina Island!

May was exhausting at times as I dealt with health issues with my parents, moving much of my personal effects off the island and working at our new transmitter site on the mainland, but things are certainly moving forward quickly. The contractors have begun to trench for our electrical power run, and though they got off to a rough start having to deal with truck and tractor repairs, things are now moving along quickly and smoothly in that regard.



I am very excited to see the new site coming to be and I believe this will be a great site for KBRT. God has opened such awesome doors for us up there it, and it leaves me in awe. We have developed a great relationship with our neighbors, especially Larry Boothe, our "next door" neighbor up on that hill, who is a great person to work with and knows the area and its history very well. Our contractors have shown themselves to be very organized and professional, something that seems to be harder and harder to find here in Southern California. I know that Cris has had his hands full with this project for a long time, another reason it is so nice to see physical work on the ground now moving forward.

One of Bill's new construction duties at the mainland site

Our transmitter plant on Catalina Island has been operating more reliably than it has in a long time. Though we have been blessed with a good quality auxiliary transmitter and back-up audio equipment including two back-up power generators, this past month all that has gone unneeded, something I can rarely say for months past. Through it all, however, KBRT has been fortunate to remain on the air though most all of the past outages, even the bizarre power brownouts that have been known to hit us several times in a week in past experiences. Soon, our new mainland transmitter site will only serve to make KBRT more robust and reliable than ever before!

Until next month, the Lord bless you and keep you; the Lord make his face shine upon you and be gracious to you; the Lord turn his face toward you and give you peace.

The Chicago Chronicles

By
Art Reis, CPBE, CBNT, AMD
Chief Engineer, CBC–Chicago

Pen Pal

About a month ago, I got an email from an unlikely source – the General Secretary and Chief Engineer of an FM multi-facility on the Shetland Islands in Scotland, one Ian Anderson (no, not the Ian Anderson who was the premiere flutist of the classical rock era). This Ian Anderson might have an even more interesting history, of which I may make mention of in an upcoming issue of *The Local Oscillator*.

For those who are, shall we say, geography-challenged, the Shetland Islands comprise a rather heavy piece of territory, weather wise, on the north edge, and I mean *edge,* of the British Isles. Next stop going north: Greenland. The station there was looking to retire an older transmitter, an Eddystone, which is a British-made rig. While the final choice was another Eddystone, they also expressed a great deal of interest in purchasing a Nautel VS-2.5. (The Eddystone, according to Ian, won by "an edge.") You readers might remember that WYCA just acquired a shiny new VS-2.5 for the Beecher site last December, so Nautel Sales gave Ian my name and said, "Just talk to him." That was nice of them, because this led to a really cool set of emails shooting back and forth across the Atlantic, from which I learned quite a bit about how radio works in the First World (Europe) and also about pirate radio, in which Ian was apparently involved back in the day.

A note about that Eddystone rig: Ian sent a picture, some three years old, of the original 1994 Eddystone rig, the one which was just replaced. That's it in the photograph, with Ian's then-10-year-old son, Bo, who looks to be an absolutely beautiful child, taking readings from it.

Bo is rather special in his own rite. He looks to be a future broadcast engineer like his father, but, quoting Ian now, "He just took the Gold in the Scottish Maths Challenge (we add an "s" to math), so he has been invited to Aberdeen University Mathematics Department for a seminar next month. He could fly down in the morning (200 miles) and back in the evening but Inga [him mom] has decided to take Bo and our 9 (nearly 10) year old Finn for a three-day break as a reward for working hard at school this past year and getting good results." Now, that's a proud dad. As for my thought, I still hope that Bo decides to become a broadcast engineer.

Back to the Eddystone: What struck me about it was its modularity. To the best of my knowledge, no transmitter produced on this side of the Atlantic was made quite like that one was made back then. Even the Italian Bext transmitters of my experience were not that kind of modular. It took years for manufacturers like BE and Harris to start designing that way. Now, of course, everyone is doing it. But I have to guess that Eddystone was the pioneer, because I believe that it was designed mainly for stations which are way out in the middle of nowhere which could afford only one transmitter. That meant a rig which could be either put on the bench one piece at a time, or sent to the factory, without it having to be taken completely off the air for other than, say, exciter failure.

Bo (age 10) and Eddystone transmitter. A really good-looking future broadcast engineer (we hope). Photo Courtesy of Ian Anderson, aka Dad, Shetland Islands Broadcasting.

European Radio is different. In some respects, British Radio is even different from

Europe. There are actually two different types of radio going on there, one which emphasizes networking, namely the big government broadcasting entities which have gobs of stations broadcasting one or just a few formats to the public; and the truly local broadcaster, which is all local live and proud of it. In the UK, the latter is a comparatively recent reality. Until the late 1960s, the BBC *was* British broadcasting, with the only competition coming from off-shore, mainly from Radio Luxembourg, and then the legendary "pirate broadcasters" such as Radio Caroline. It was the popularity of those pirate broadcasters which caused the BBC to see the light, change the way it did business, and let the British listening public have what it really wanted. Not long after, opportunities for local radio became available, which then led to the creation of Shetland Islands Broadcasting, and many other privately owned stations like it.

Today, the changes are coming not so much from ownership and format considerations, but rather from technical ones, and of course that means digital. As anyone who is heavily into this business knows, digital in the European mainland means less Ibiquity (if there is any at all) and much more Digital Radio Mondiale (DRM). Even Nautel, which touts that they are the one who make HD work, are also into DRM in Europe. Don't expect it here anytime soon. Digital Radio Mondiale means what it says – digital – and it was never designed to co-exist with any co-channel "stinking analog" at all. Stations using it can broadcast up to two program sources on a channel (compared to Ibiquity HD's four, at present, and growing); however, according to Ian, the UK is already committed to the DAB (digital audio broadcast) system, based up above 226 MHz, and capable of multiplexing up to 10 different simultaneous program channels. That's wideband with a capital W. I wonder what the bandwidth of the individual program channels is. I'll have to ask.

Even with that, the UK is allowing local broadcasters who wish to do so, to stay FM for now. However, the big national networks (the BBC et al) are already planning to abandon both of the analog technical formats, AM and FM (AM, already pretty much shutting off in the European mainland, will eventually go the same way in the UK; the writing was on the wall when BBC-2, the Long Wave service, was shut down some years ago).

This has me asking, "Would such a thing happen here, in that way?" I think so, but not in the near term. We Americans still find analog AM, for instance, to be quite useful, especially in the areas of talk radio and sports broadcasting. Will digital finally gain acceptance in the marketplace? I believe so, now that the public is starting to become aware of the differences between HD and satellite radio. Remember, is took from 1936 to 1975 for FM to get to parity with AM radio. Comparatively speaking, HD is moving a lot faster than that. True, multicasting will help a lot, but acceptance for dumping analog will be slower on this side of the pond than it is "over there," simply because we as a nation are not "wired" into foisting that kind of change on the public, in the way that they do it in Europe.

Wait a minute: Is *that* even true anymore? Anyone and everyone who is into computers, iPods, iPads, TV and personal phones of any brand should already be quite used to the concept of having to change technology every so often by now. After all, the manufacturers of all this digital hardware have been foisting their changes onto us for years. And don't look now, folks, but we've been *buying* it! Hmmm…. a precedent, maybe? Maybe we *are* more amenable to accept and maybe even embrace such change under those circumstances, as the Europeans have already done.

I didn't say I liked the concept. Don't ask me to. Not right now, anyway. I'm still "old school." But I suspect that when all is said and done, sooner rather than later, given the European experience, that might end up being how radio eventually changes on this continent. We'll see.

Things for Which you Should Not Use the Internet, Part 2

Let's pick up where I left off regarding the Barix Internet transmitter/receiver system being used to provide radio format programming over the Internet (supplanting satellite). Last month, I said the following: "In my experience, the Internet is not ready for this type of prime time; that is, being the conduit for long form radio or television… programming to affiliates." I'm not alone in my sentiments. Andrew Thomson, Customer Service Representative for Barix Technology, Inc., based in Switzerland, in a recent email responding to my inquiries on the subject, said, "As you had said, sending a stream 24/7 over the Internet can be a dangerous prospect if a node gets overloaded or cannot support the amount of data you are sending… The Exstreamer 500s do have four [control] inputs and four dry contact closures on each unit which could be used to trigger automation systems instead of tones. If something is happening to the tone either via compression or from packet loss, it could very well not get picked up by the automation system and

put on the air."

The thing is, there *are* DTMF tones being sent at the time of the break beginnings, but with the control signals being sent as digital words, why are they there? To this point, I have no clue and apparently neither does Andrew Thomson of Barix. It makes no sense to use analog anything as a controlling medium on the Internet. As of this writing I've yet to discover the means by which to reach the Mex-Mix format in Orlando, or I would ask the CE there. That's a project for later.

A final note: I wish I could have helped that station more. I must admit that I didn't do very well in my efforts to deal with the situation this time. They did get the problem straightened out, but by their IT person, not me. Other opportunities to deal with stations that have formats being distributed via the Internet will doubtless be coming along. Using that medium for that sort of thing is apparently inevitable. For my part, at the present state of the art, I would prefer to take a pass on it, were it my station. Later, when the Internet becomes better developed, maybe I might, but not for now.

Until next month, blessings to you all!

The Portland Report

By
John White, CBRE
Chief Engineer, CBC–Portland

Memorial Day

Over the years, many have come to think of Memorial Day as a three-day holiday, the start of summer and other superlatives that miss the point. The most direct route to Mt. Scott passes the Willamette National Cemetery. Each year the Boy Scouts place the sea of flags that mark those that rest there.

As I think back this Memorial Day, I remember my grandfather, John Henry, who fought in WW1, my father who was building military aircraft at Douglas Aircraft on December 7th, 1941 and my uncle Jimmy on board the Destroyer Blue at Pearl Harbor.

This year, attendance was way up at Willamette National. On 111th the line was to the bottom of the hill, 1.5 miles with similar backups east and west bound on Mt. Scott Blvd.

As I was seeking an opportunity to take an alternate route, I recalled something Colin Powell had said. When in England at a fairly large conference, Powell was asked if our plans for Iraq were just an example of empire building. Powell answered, saying, "Over the years, the United States has sent many of its fine young people into great peril to fight for freedom beyond our borders. The only amount of land we have ever asked for in return is enough to bury those that did not return."

I will have further thoughts below the fold.

A Second Opinion

I wanted to take a moment to comment on the common phrase, second opinion. We all know the advantages in complex medical situations. I am now considering the usefulness in other situations. A week ago, the AC portion of the HVAC system failed at Mt. Scott.

The first symptom I noted was a ground fault with the floating delta circuit. One of two phases showed alternating phase faults to ground, although that failure doesn't cause a tripped breaker failure. The second symptom I noted was the compressor unit was off line. No hint of activity. I checked the typical failure modes: a cartridge fuse open, high head trip, and open activation circuit. None of those were the problem, so I called in a service tech, who arrived with all the needed test equipment. He told me that he had swapped the contactor, which didn't fix the problem. He said the condenser fan ran slow (growled?). He also said he tested the compressor motor resistance, which showed to be open.

The reason I questioned the info is that everything the service tech said can point to power

problems. I can't believe both the fan and compressor would fail at the same time. His swap was the contractor, again suggesting he thought it was a power problem.

All that coupled with the phase fault to ground suggested to me a power problem and not a compressor failure. This is an older unit, so a problem with the condenser fan motor could be easily repaired while a compressor problem could not. Therefore, knowing the precise cause of the problem is important.

As a follow up, I contacted a friend who has industrial experience with three-phase power and HVAC systems. He brought his air conditioning test equipment and we went through the compressor unit piece by piece. We found that the condenser fan, a ¼-horsepower single-phase motor, had a mid-winding fault to ground. With the fan disconnected, we are getting indications that the compressor is working normally. Our next step is to bring in a box fan to provide temporary condenser cooling so we can test the compressor under load. It looks so far that this second opinion will pay off big time.

Some Final Thoughts

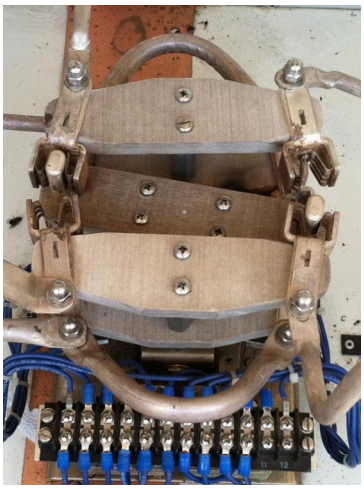
I had wanted to say more about Memorial Day but found that Abraham Lincoln had said it better in fewer words. I will let President Lincoln and the Gettysburg Address say it for me:

> "Four score and seven years ago, our fathers brought forth on this continent, a new nation, conceived in Liberty, and dedicated to the proposition that all men are created equal.
>
> "Now we are engaged in a great civil war, testing whether that nation, or any nation so conceived and so dedicated, can long endure. We are met on a great battlefield of that war. We have come to dedicate a portion of that field, as a final resting place for those who here gave their lives that that nation might live. It is altogether fitting and proper that we should do this.
>
> "But, in a larger sense, we can not dedicate – we can not consecrate – we cannot hallow – this ground. The brave men, living and dead, who struggled here, have consecrated it, far above our poor power to add or detract. The world will little note, nor long remember what we say here, but it can never forget what they did here. It is for us the living, rather, to be dedicated here to the unfinished work which they who fought here have thus far so nobly advanced. It is rather for us to be here dedicated to the great task remaining before us – that from these honored dead we take increased devotion to that cause for which they gave the last full measure of devotion – that we here highly resolve that these dead shall not have died in vain – that this nation, under God, shall have a new birth of freedom – and that government of the people, by the people, for the people, shall not perish from the earth."

Rocky Mountain Ramblings
The Denver Report
by
Amanda Alexander, CBRE
Chief Engineer, CBC - Denver

Day/Night Issues

May was filled with many issues it seems. The day/night switch for 670 KLTT has begun giving us fits again. This time, however, not just at pattern change time. The switch will actually go fine, but sometimes several minutes later, the interlock will open and take the station off the air. When this happens, I will get a call from the board op on duty at the time and then rock the day/night mode to get the station to come back up. Sometimes it works and a few minutes later, it will go back down. Making this issue happen during the day is a difficult task because the tower lights are all off and going around turning everything on would be difficult. I did go to the site and attempt to reproduce the issue to no avail. I did see that some of the switches were not making great contact.



One of the RF contactors at KLTT.

The problem disappeared for awhile, so I figured maybe it fixed itself. That is always a worry because the question isn't *if* the problem will occur again, it's *when*. Well, on May 29, it came back. At 8:12 PM I got a call saying the station was off. I knew immediately what to look for. I rocked the day/night mode and got the station back on air.

The issue at this point has got to be one of the microswitches on the RF contactors either not being fully depressed after actuation or the switch itself is faulty. The trick is to figure out which one without leaving the station off the air long enough for me to drive out there and see. So the next step will be to install a web cam at the site to watch the tally lights on the phasor controller to tell me what tower/switch is giving me grief.

Backup ISDN

Another issue that occurred last month at KLTT was actually a simple thing to fix. The Ethernet switch on top of tower #4 got its brain scrambled (in clear weather), and that took out the Ethernet path from the studio to the transmitter (and killed the audio feed from the Intraplex). As soon as I figured out what was going on, I tried to dial the station up on ISDN using the Zephyr XStream. But that didn't work. I had to rush out to the site and power cycle the AC power to tower #4, and that cleared whatever was wrong with that six-port switch that connects to the Trango microwave link and the Ubiquiti NanoBridge link to the building. While that got the station back on the air, I noticed that the ISDN backup was not working properly.

The next day I went back to KLTT to look into this. I'd dial the ISDN up and it never connected with audio. We had one Adtran ISDN unit left, so I went to KLZ the next morning to grab it and installed it at KLTT. I was seeing a transmit signal when nothing was being transmitted, so we naturally thought the ISDN unit was bad. But that wasn't the case. To verify, I connected the KLTT Comrex DXR.1 codec to the Adtran ISDN unit at the KLZ site and that worked fine. I also connected the KLTT Adtran to the KLZ codec with similar results. So back out to KLTT I went with codec and Adtran.

The problem, which took a little while to figure out because the green "Ready" LED on the KLTT DXR.1 was dim and hard to see in the fluorescent light at KLTT, was that the "relay" output of the DXR.1 was not closing when the "Ready" light would come on. It didn't take long to figure out that an opto-isolator (U17) in the DXR-1 was bad. I was

able to find a replacement at Mouser and got some spares as well for the other two DXR-1 units we have. I replaced the opto and all works fine now.

Network Issues?

Do you remember the sporadic issue we had a couple of times at KLZ with the audio all of a sudden cutting out and us not having any luck figuring out why? The problem was clearly data-related; the microwave path was solid and we had no lost or dropped packets on that path, but something was happening between the tower and the building, something apparently other than the NanoBridge link (which also showed zero lost/dropped packets).

A few months ago we replaced the network switch on the tower thinking that would solve the issue. Perhaps that did make a difference, but the same issue happened on KLDC on the 22nd. I was actually heading out to KLVZ to meet Brighton Fire for our yearly inspection when Randy Frongillo called me to inform me of the issue with KLDC. I immediately called Keith Peterson and had him head out to KLVZ while I stopped at KLZ.

That fire inspection isn't a big deal, so I decided not to lug my laptop with me to the site and as such, didn't have it with me. The KLZ site has a computer on the studio network that I could use, so I stopped in there. I immediately noticed the studio Intraplex was losing packets by the thousands every second. So I rebooted the CM-20 Intraplex cards at the studio and at the transmitter. When they came back up… nothing. Next, I decided to reboot both Canopy units on the studio-to KLDC path and then the Intraplexes again. Still nothing.

By this point I was really frustrated. I knew the station wasn't losing money at this point because we were in a music segment, but any off air time is bad. People start tuning elsewhere on the radio dial. So I decided to head straight to the KLDC transmitter site.

When I got there I did the same thing I had been doing, rebooting everything. This usually worked for KLZ so why not KLDC? Still nothing. At this point I was thinking interference. To look at the spectrum I needed a laptop and needed to be at the transmitter site to have access to it. So I headed back to the office. I decided, just for kicks, to go physically pull and reset the CM-20 card from the studio Intraplex (as opposed to doing another software reboot as I had been trying). And what do you know… everything came back up the way it should! We were still losing packets, but instead of thousands it was just a few every few minutes. Still not perfect, but the station was back on the air. We have not had another issue with since.

We have continued to see lost/dropped packets on the Intraplexes for all the other stations as well. Again it's not a lot, just one or two every now and then, but we shouldn't be losing any. The Trangos, the Canopy and the NanoBridges all show perfect throughput, so I don't think the problem is in the over-the-air segments. After discussing this with Stephen Poole, we all agreed this sounds like a network issue. The switches we have the Intraplexes connected to are old. I am awaiting approval to get a new gigabit smart switch to replace those two older ones at the studio. We'll see if this fixes our issues permanently. If not, we may start replacing Intraplex power supplies to see if perhaps they are generating noise that is causing the problem. All are about the same age, so if one is giving problems, chances all are (or soon will).

Time to Mow!

We were able to get our brush hog welded in May. Years of it being beat up by rocks and other debris caused the top skin and the frame to separate in some areas. General contractor extraordinaire Mike Kilgore was able to patch it up using our arc welder and get it looking and working great. I ran a test through the KLZ antenna field afterwards and found it works great. Hopefully this fix will last several years too.

Mike Kilgore welds the brush hog deck.

That about wraps it up for this edition, so until next time… that's all folks!!!

Digital Diary
by
Larry Foltran
Corporate Website & Information Technology Coordinator

Siri's Eyes and Ears

If you've read the technology related news section lately, you may have noticed a small blip of a story relating to IBM's ban of Siri enabled iPhones from their facilities. Despite being a sideline type tech story, the overall response has truly intrigued me. Is this a knee-jerk reaction to new technology or are there valid privacy and business security concerns?

This type of move is certainly not new. Some of you may recall the National Security Agency's (NSA) ban of the robotic Furby toys back in 1999. Aside from being extremely annoying – trust me, we had two in our house at the time – the NSA was concerned that these toys held the potential to "listen" and then repeat classified information. Despite what was claimed in the advertising campaign, Tiger Electronics, the company responsible for these toys, quickly downplayed the concern in stating that their toys were unable to actually learn words. In fact, they were pre-programmed with roughly 100 English words which would slowly replace the toy's odd "Furbish" language. Even after the manufacturer's quick explanation of the technology behind the Furbys, the NSA maintained their stance on the ban. Quite honestly, I don't blame them and it has nothing to do with the potential for a security breech. The novelty of these things communicating with each other quickly disappeared after about a week and the batteries were ultimately removed.

Fast forward a few years to the point when cameras were becoming standard equipment on most cell phones. Once again, privacy became a concern and bans of such items were put in place in public gyms, courts and a variety of businesses. I recall the company I worked for at the time announcing that cell phones equipped with cameras were strictly forbidden within the building. In some cases, those with camera phones were required to check their devices in with security at the front desk or acceptably cover the camera lens in some way. Some co-workers went so far as to physically remove the camera from the phone. It was obviously recommended that employees purchase only phones without cameras, although at the time it was already becoming quite difficult to do so. I'd be surprised if you could even find a model without a camera today.

So in 2012 we again find mobile phones at the center of potential privacy concerns with Siri on the hot seat this time around. Again I ask, is there a valid concern? To determine this, we first need to dive into what type of data Siri collects. The first indication comes from Apple's iPhone user license agreement. You know, the long legalese thing we typically accept to get on with using the item or software? Their agreement specifically states that information provided or accessed through Siri is recorded and sent to Apple's server, potentially their enormous data center in North Carolina. This includes your contacts, dictated information and other data that you store on your iPhone. According to Apple, this is done only to improve Siri's responsiveness.

The true level of security concern is relative to how the user utilizes Siri overall. I'm fairly certain that most users could care less that Apple's servers hold data about their favorite music, restaurants, or how often they check the weather. The real concern lies within those using the dictation function to compose emails or text messages. The system doesn't differentiate between confidential and general content. Everything is stored on the server which leads to two other very important questions. How long is this data stored for and who has access to it? Apple has remained mum on both counts. Although if its approach is anything like that of Google or Facebook, your information will be on their servers for a very long time.

The reality is that personal data is collected in transmitted in numerous ways every single day in varying levels. In some ways it's input by the user such as social media, search engines, or numerous other avenues. Even data considered mundane is recorded and stored. As an example, it was recently reported that Facebook even keeps track of events you've been invited to and whether or not you

planned to attend these events. In other ways, it's simply part of the technology we use such as GPS location identification within smart phones. I'm eager to see whether general consumers will simply accept the fact that their lives have become an open book as they use these technological tools or if there will be a backlash as privacy concerns gain traction. The privacy concerns related to Siri have already prompted the ACLU to issue a general warning and may continue to expand.

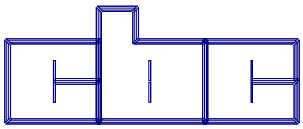
Whether the data collected is used for anything other than what Apple claims is yet to be seen. I do foresee some companies following in the IBM's steps simply as a preventative measure. The "better safe than sorry" game plan similar to what was used towards USB flash drives some time ago by a variety of businesses.

The other side of the coin will be the average user utilizing this tool for non-business purposes. Given the fact that you can trace Siri's lineage back to the US Defense Advanced Research Projects Agency, commonly referred to as DARPA, some users would extremely concerned that their iPhone is recording everything they do. Trust me this is a true concern for some users. I recently had a long and somewhat comical discussion with one person relating to Siri's role in domestic spying. Concerned users do have the option to disable Siri via the general settings menu. According to Apple, doing so will delete any recent user associated data. But will this be enough for some folks? I suppose the ultimate question is whether or not these folks feel they can live without Siri.

…until next month!

KBRT • Avalon - Los Angeles, CA
740 kHz, 10 kW-D, DA
KCBC • Manteca - San Francisco, CA
770 kHz, 50 kW-D/1 kW-N, DA-1
KJSL • St. Louis, MO
630 kHz, 5 kW-U, DA-2
KKPZ • Portland, OR
1330 kHz, 5 kW-U, DA-1
KLZ • Denver, CO
560 kHz, 5 kW-U, DA-1
KLDC • Brighton - Denver, CO
1220 kHz, 660 W-D/11 W-N, ND
KLTT • Commerce City - Denver, CO
670 kHz, 50 kW-D/1.4 kW-N, DA-2
KLVZ • Denver, CO
810 kHz, 2.2 kW-D/430 W-N, DA-2
KSTL • St. Louis, MO
690 kHz, 1 kW-D/18 W-N, ND
WDCX • Rochester, NY
990 kHz, 5 kW-D/2.5 kW-N, DA-2
WDCX • Buffalo, NY
99.5 MHz, 110 kW/195m AAT
WDJC-FM • Birmingham, AL
93.7 MHz, 100 kW/307m AAT
WEXL • Royal Oak - Detroit, MI
1340 kHz, 1 kW-U, DA-D
WLGZ-FM • Webster - Rochester, NY
102.7 MHz, 6 kW/100m AAT
WRDT • Monroe - Detroit, MI
560 kHz, 500 W-D/14 W-N, DA-D
WMUZ • Detroit, MI
103.5 MHz, 50 kW/150m AAT
WPWX • Hammond - Chicago, IL
92.3 MHz, 50 kW/150m AAT
WSRB • Lansing - Chicago, IL
106.3 MHz, 4.1 kW/120m AAT
WYRB • Genoa - Rockford, IL
106.3 MHz, 3.8 kW/126m AAT
WYCA • Crete - Chicago, IL
102.3 MHz, 1.05 kW/150m AAT
WYDE • Birmingham, AL
1260 kHz, 5 kW-D/41W-N, ND
WYDE-FM • Cullman - Birmingham, AL
101.1 MHz, 100 kW/410m AAT
WXJC • Birmingham, AL
850 kHz, 50 kW-D/1 kW-N, DA-2
WXJC-FM • Cordova-Birmingham, AL
92.5 MHz, 2.2 kW/167m AAT

CRAWFORD
BROADCASTING
COMPANY



Corporate Engineering

2150 W. 29th Ave., Suite 300

Denver, CO 80211

email address: crisa@crawfordbroadcasting.com