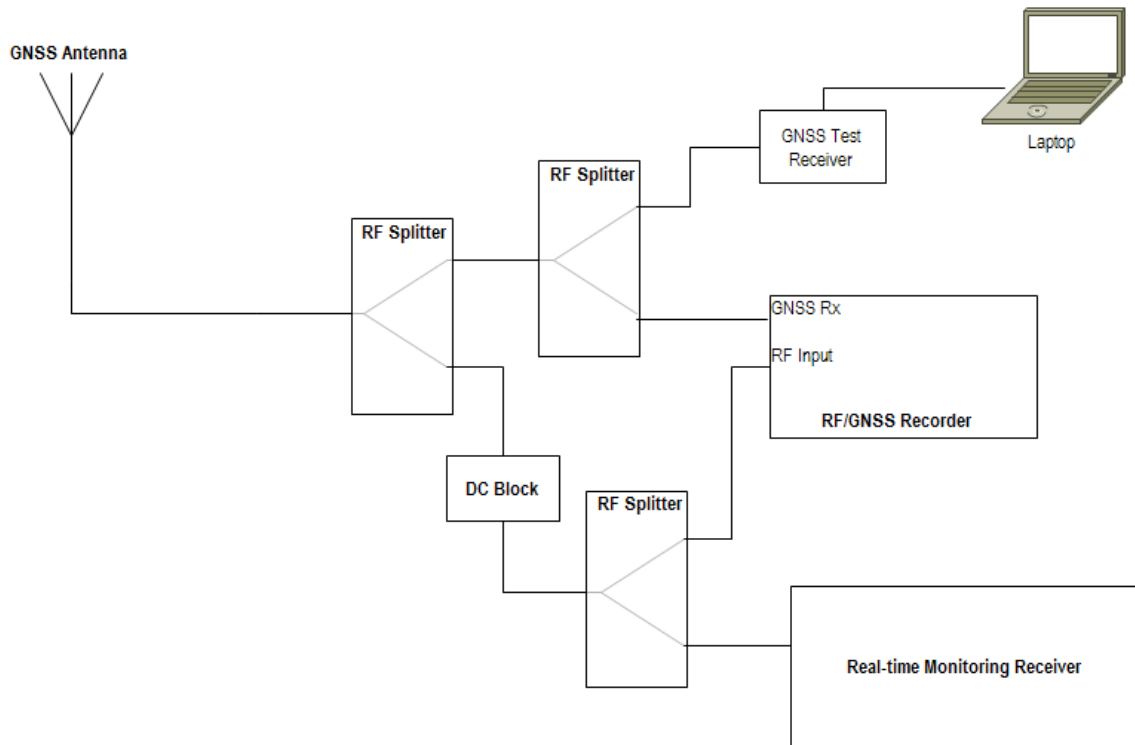


GNSS Jammer Observations:

Setup:

For this study, a vehicle was outfitted with a real-time monitoring receiver, RF/GNSS Recorder, and a GNSS test receiver running on open UI on position and satellite receiver strength. It was important to assure authentic and realistic GNSS receiver signals were captured in this environment. All signals were observed and captured through a signal split from the GNSS receiver active test antenna. This enabled a good noise figure and tuned passband for the GNSS signals and reduced potential overloads from nearby transmitter towers (ATC radar and cell towers). Even with the splitter losses, GNSS signals were able to sync with the test receiver in less than one minute from a cold start.



Purpose:

The mission is to collect jamming signals and get good digital IQ recordings in a real-world environment. The test methodology employed in the cell phone industry, LBS (Location Based Service) test scenarios are developed for the field-to-lab conformance testing on their networks. As it is necessary to continue to assess and evolve the GNSS receiver industry with realistic test scenarios observed in the field, a similar field-to-lab collection of RF signal impairments are observed. This plays in nicely to the new ION charter that Sanjeev Gunawardena (Ohio University) has for standardizing the formats of raw data collections (XML metadata descriptions). Having a set of expected test scenarios allows a lab based assessment of Rx performance. It also enables GNSS receiver developers to harden their products, if they choose. It is much more cost effective to have good recordings that can be played back in a lab than the expense of testing products in the field for the first time at an event like NAVFEST.

Observations:

With over a dozen recordings performed so far, collections had mainly concentrated on driving around an office park environment in Beaverton, OR, a suburb of Portland. For this set of collections, the starting point was the PDX Cargo Area (Portland International Airport). While several "signals of interest" (SOI) had been observed in prior collections, identifying SOIs became much more intuitive with the added incorporated a separate real-time monitoring receiver for this latest collection.

The real-time monitoring receiver was important to eliminate the multitude of false trigger signals and provide a real-time signal to observe in frequency, power vs time, and frequency over time (spectrogram). It also provided feedback to understand if the satellite dropouts were environmental (shadowing from a

building, truck, or bridge) or radiated RF energies. (Our simple low-end record/playback solution is essentially faceless with a very low update rate of the RF spectrum display).

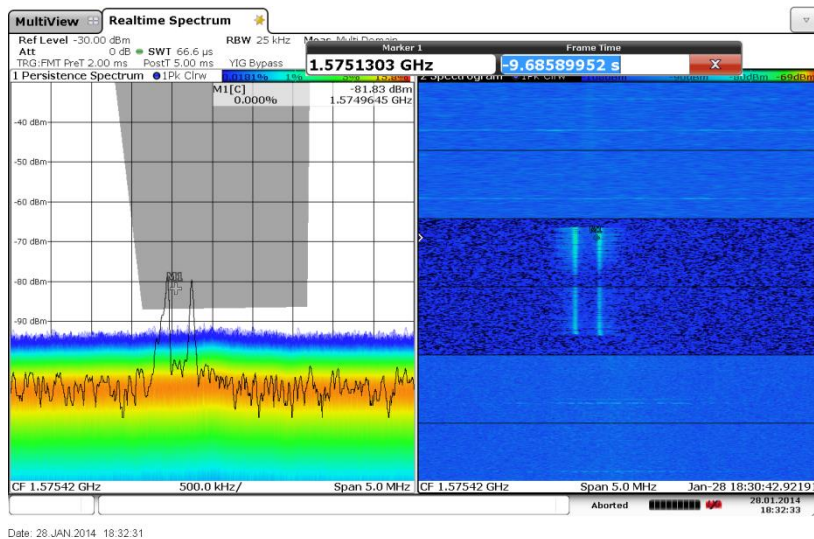


Figure 1 – Most common “false SOI” – the Key FOB FSK signal trigger with spectral mask (~3m duration sets of FSK signal repeated up to five times 100 ms apart over 0.5 second period)

As demonstrated at the ITM 2014 event, the 5th harmonic of the 315.15 MHz Key FOB’s were the most recorded signal. The effect can be temporal, and some potential dropouts were observed around the PDX parking structure due to the sheer number of events occurring during the drive. Garage door openers and other ISM band licensed devices fall in this category and the observed behavior is easy to identify. (Might want to make sure a GBAS system is not located near a parking garage.)

The real interesting observations started when in stationary position in a parking lot along the HWY 30 Bypass linking PDX to the Highway I-5 corridor. For about a half hour around 11:00am, RF observations were made while parked in a fixed position as vehicles passed one at a time either East or West bound along the single lane corridor. There were so many events of interest over a 10 minute period, it was decided to collect on a moving target. Approximately every third or fourth truck appeared to have a spectral signature of interest. **There was no attempt to determine if these signals were intentional or unintentional**, just track signals of interest. The fact that so many trucks that passed by this area with high levels of spectral emissions could also relate to an EMI problem with the electronics on board of the passing trucks (ex. radio booster amps).

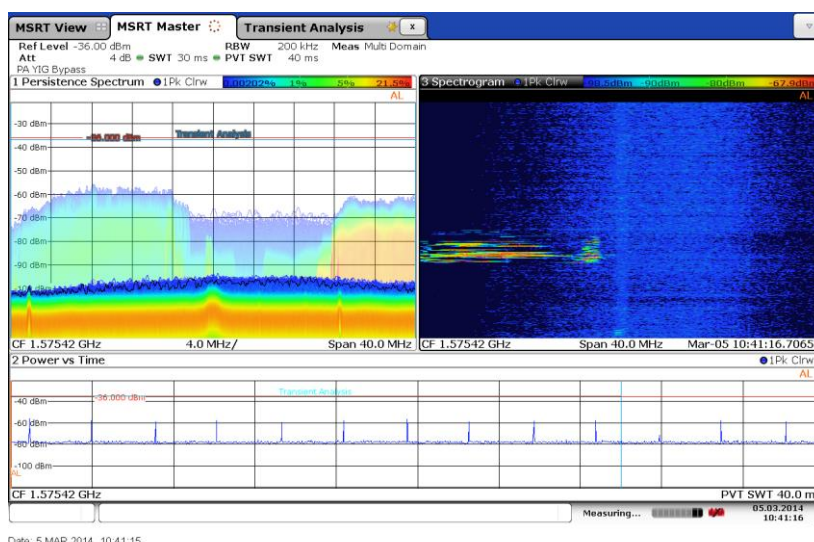


Figure 2 – Example Signals of Interest during parked observation (notice the offset from center frequency in a 40 MHz span) – Spectrogram event shows SOI lasting about 1 second.

While it was evident that these signals would be large enough to possibly desensitize our GNSS receiver, only temporal dropouts were noted as they RF signals drove by at 30-40 mph. These events were only in the range of the antenna for less than a second. Also, with our center frequency clearly on L1, and our span at 20-40MHzit seemed that many of the SOI were centered several to 10's of MHz away from L1.

Fixed on a setting of 20 MHz span, a real-time spectrogram display of a couple seconds, a Power vs time view to look for periodicity; the collections were now made in a mobile environment to pursue a signal of interest that could be seen in the distance (figure 3).

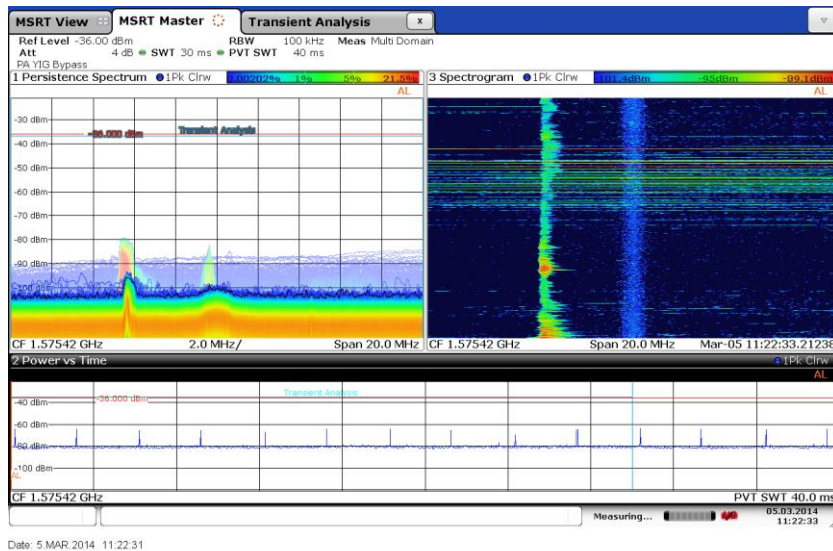


Figure 3 – Signal of interest at a distance. Blue trace on spectrogram is L1

It was easy to associate this signal with a double tandem trailer truck driven by someone from our local waste management company here in Portland. We saw the signal similar to figure 3 for several minutes while the vehicle was trailed at a distance. The double tandem trailer was near 100' long.



Travelling behind the trailer for several minutes, the GNSS receiver never lost lock (jamming signal out of band a few MHz). When entering Highway I-5, it was now possible to move alongside the truck.



Collections continued along the trailer side in an open lane passing very slowly, it wasn't until reaching the first trailer that to lose GNSS satellites began to lose lock. Observing the difference between truck shadowing and RF jamming was now intuitive in the GNSS test receiver user interface. Then, the signal changed (Figure 4)again and again.

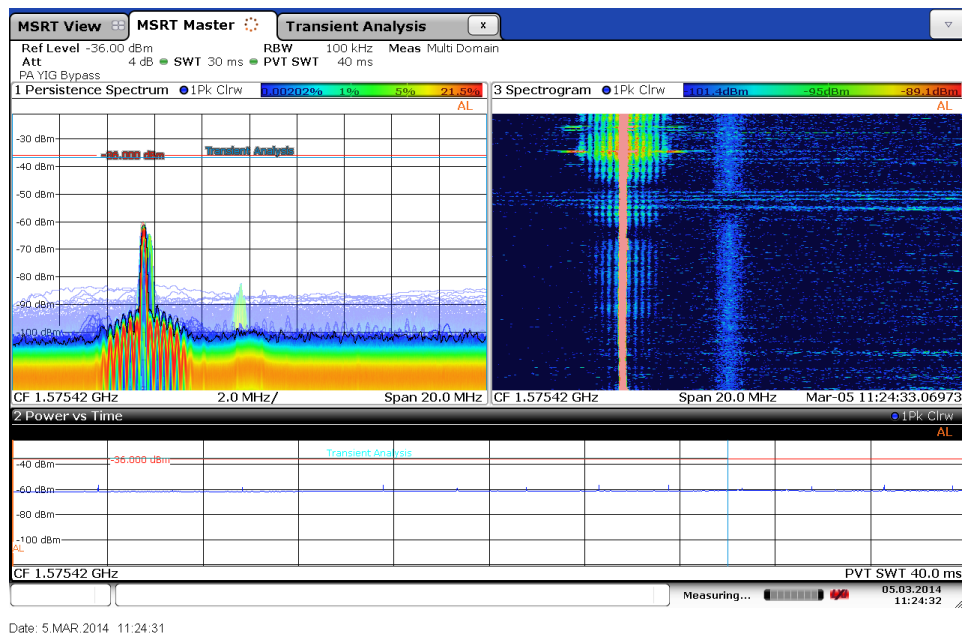


Figure 4 – Mode change while traveling alongside truck

Over the next several minutes, collections continued along the side of the semi-cab while our GNSS receiver remained completely jammed.

Several mode changes were documented while driving next to the cab for these few minutes as can be seen from the timestamps on the screenshots.

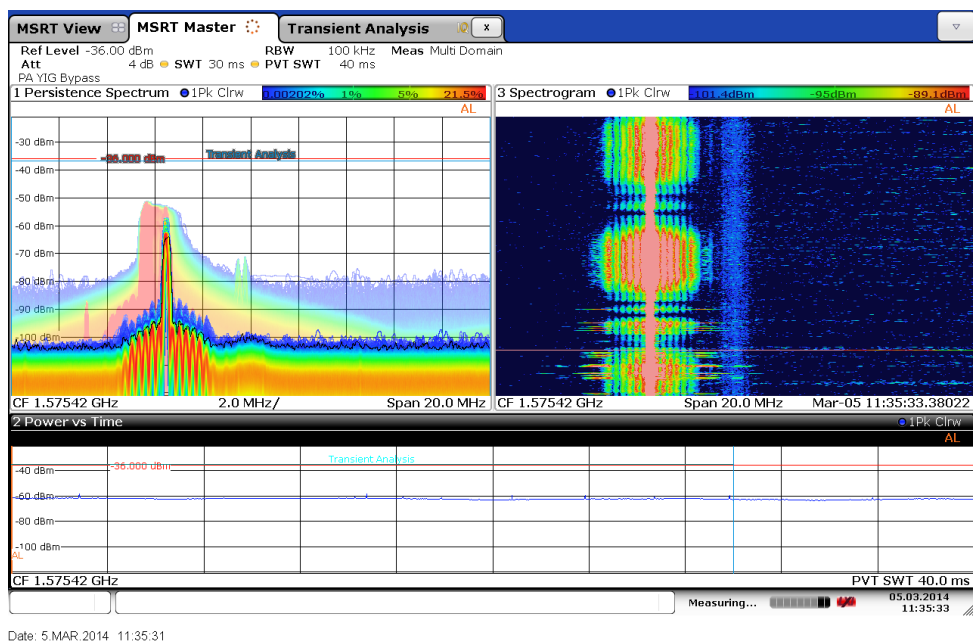


Figure 5 – Pulsed mode of operation – centered out-of-band for L1 C/A, but inband for L1 Y code.

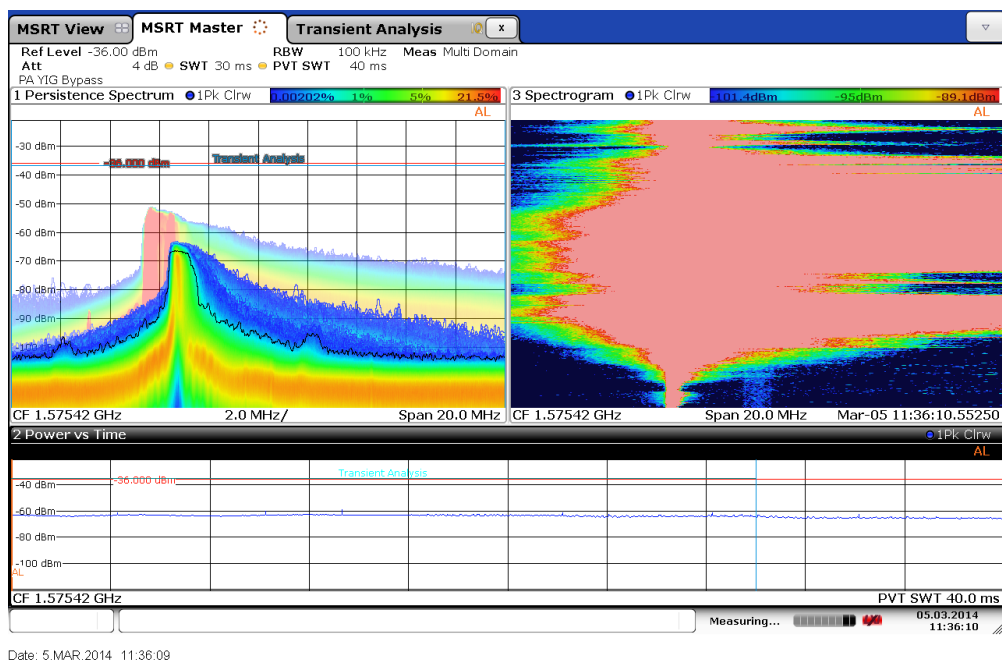
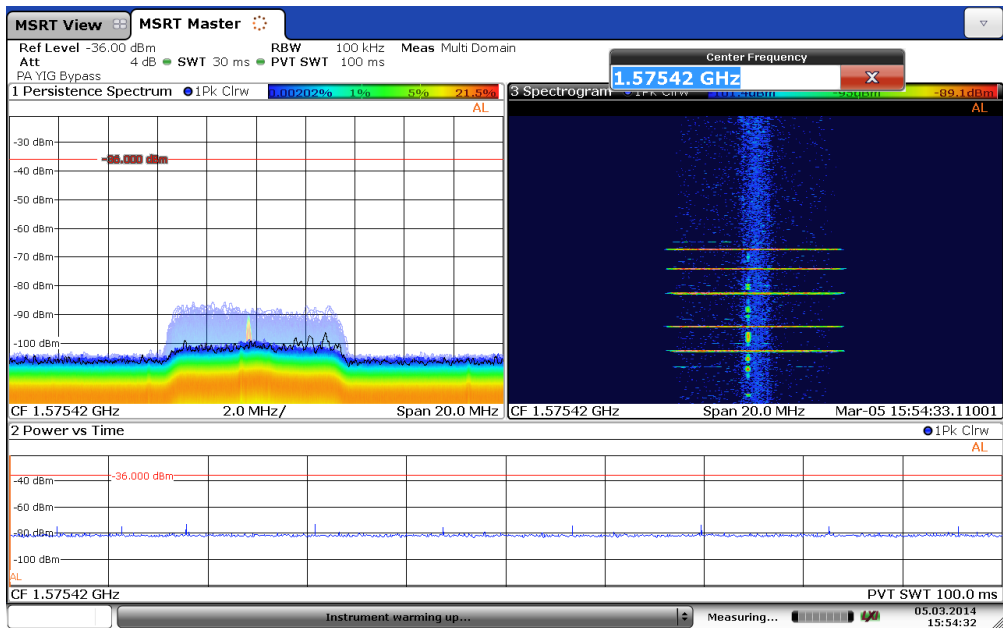


Figure 6 – Slow Chirped CW mode of operation 38 seconds later

Summary to date:

Several more runs are needed to improve the collections. Initially it was believed that a 7.5 MHz recording would yield correlated results to observed RF environment.



Date: 5.MAR.2014 15:54:32

Figure 7 – Playback of the Pulse mode in 7.5 MHz bandwidth

Upon studying the signal playback through with similar setting to the monitoring receiver, it is easy to measure the results inband (PRI), however, the replay, which included the metadata of the GNSS recording in a narrow bandwidth, did NOT yield the impairments observed in the actual receiver during the field test. A wider bandwidth recording is necessary for this type of signal if it is desired to recreate the field environment in the lab.

Also, the signature signals observed with the Slow-Chirped CW and the Pulse mode always seemed to be off center of the L1 frequency by several to 10's of MHz. Based on an unscientific observation here, this only had the effect of jamming our GNSS receiver completely when we were within 50 feet of the cab. If this was an intentional jammer, this would have the desired effect of jamming the GNSS receiver in the semi-cab, with only minimal impact to the nearby users of GNSS signals (tuning the area of impact). If this signal is unintentional, then it would seem to be a very challenging signal environment for the L1 signal. Future studies must also include concurrent signal analysis at L2 and L5. L2 signals were also lost during this event on the GNSS test receiver, however no recording were made of the RF environment.

The spectral shapes give insight on the method of isolating this type of signal in the future. The fact that the modes change (waveform diversity) poses an interesting challenge for automatic detection.