Yaesu Repeater Lockup

Category: Fusion,Troubleshooting
December 23, 2024
It is well documented that the Yaesu DR-1X and DR-2X repeaters can lock up from time to time. When they lock up, they may:

- Not respond to any transmission or control function and
  - Transmit continuously or
  - Not transmit or
  - Transmit for the duration of the time-out timer, go off the air, key up and start all over again.
- The transmission may be digital “noise” or it may be a carrier

There is another form of lock-up in which an attached HRI-200 can be used to reset the repeater.

Why do they lock up?

We don’t know for sure why this happens as we don’t have access to the source code of the repeaters. But guesses can be made from knowing what the problem is, how microprocessor and their software works, and the common mistakes programmers make.

The firmware consists of a number of modules that do specific tasks. Data is sent to a module, the module may call other modules, and it returns with possible data. The input data may contain values that are out of range for the module. For example one value might be mode where 0=FM, 1=DN, 2=VW, and 3=VW. But what if the module receives a 4? It should just stop and return to the calling module with an error indication. Most likely the solution will be to ignore the request and stop processing. That’s what should happen. But a sloppy programmer may NOT VALIDATE INCOMING DATA and allow the ‘4’ to be processed where

the results may be unpredictable since no code was written to handle this case. There is good evidence that Yaesu software and firmware DOES NOT VALIDATE INCOMING DATA resulting in an UNHANDLED EXCEPTION.

There are other types of invalid data which should not be processed. The Fusion digital data might have uncorrected errors in it, thus it's impossible to know what the correct values are. A field of data that is sent may be longer than it should be. This problem is commonly known as a BUFFER OVERFLOW. There is some evidence to support that a buffer overflow is occurring. Since the receiving buffer must be limited in size, too much data may cause the firmware to overwrite values that are past the end of the buffer. These may be critical values that are needed for the correct operation of the repeater.

The repeaters use a real-time operating system. An RTOS is event driven and will perform a function when an event occurs such as a timeout, a signal received, a clock tick, a button push, etc. There may be cases where two events are related such that one must occur before the other. For example, one event may lock access to a hardware resource and the other event clears it. If the order were reversed the hardware resource would never be accessible and the actions of the hardware may be unpredictable or stop altogether. This is known as a RACE CONDITION. It is very likely that this error exists in the firmware and that it may be combined with another firmware error. For example, a BUFFER OVERLOW may result in a RACE CONDITION which the engineers did not see.

As a result of the above firmware problems, it is not easily predictable what the microcontroller may do next. Some systems include a Watchdog Timer. This is a hardware timer that is set for a certain period of time, perhaps 10 seconds. The microcontroller's firmware periodically resets the WDT if it is

running properly. If the WDT times out due to some sort of problem, the hardware resents the controller. We have some evidence that Yaesu has implemented a WDT in the DR-2X repeater. It is therefore apparent that the WDT has been turned off, set to a crazy long value, or that the modules that reset the timer are still running even though nothing else is.

A SOFT LOCKUP may occur if a RACE CONDITION removes access to the receiver and/or transmitter. While the repeater won't receive or transmit, the other functions are working. This means the repeater can be reset without needing to cycle the power. (There is no reset button like on your PC.)

The Evidence

The most difficult problems to fix are the ones that almost never happen. These lock-up problems are in the category of infrequent but very high risk (a drive to the mountain to reset the repeater. With remotely-controlled repeaters, a lock-up is an unacceptable risk. After all, other repeaters don't seem to have this problem.

(There is a repeater bug involving the CWID on FM, that is not being discussed here.)

It is very likely that these problems occur while a user is transmitting in the digital mode. We've not been able to observe a repeater suddenly locking up without some sort of input to key the transmitter. (However, since we haven't seen it doesn't mean it doesn't happen.)

My observations are that this is more likely to happen when a user is transmitting a WiRES-X command such as changing rooms.

It appears to be more likely if the user has a weak signal into the repeater.

It is more likely to happen on two meter repeaters than on 70 cm repeater.

Notice that each of these conditions have the word “likely”. That’s because there are unknown additional parameters which may be involved. For example, a weak digital signal will cause more digital errors. A particular error may be involved in creating the problem.

It may also be the result of a transmission starting at the exact time the microcontroller is performing a specific function, thus resulting in a RACE CONDITION. This problem is virtually impossible to observe.

It was previously mentioned that using a two meter repeater makes this problem more likely. The issue here is the amount of noise on the two meter band. All of our electronics and networks add noise to the environment. This noise level is much stronger on two meters than on UHF. There is also some evidence that the ethernet cables can deliver RF to the ethernet devices and these devices may act like a mixer. All of this causes more noise making stations effectively noisier. The end result is more bit errors and buffer overflows.

What to do?

The correct answer to this section is to have Yaesu fix their bugs in the microcontroller – but don’t hold your breath. This could be a very costly to find the cause since it is difficult to reproduce. Another problem is that there are no Fusion repeaters in Japan. (Only D* is allowed – that’s along story.) Thus the Japanese engineers working on this project would have no way to experience the problem. (The repeaters can only be operated in a shielded room – thus no noise.) I’ve solved problems like this before and the first step is to make the

problem happen more often while monitoring the CPU. Keep trying things until the probability of a lockup increases, then try doing more of that. The business model for this is that spending a bunch of money on this is not likely to sell more radios. I also believe that Yaesu farms out certain tasks, like firmware development, to outside suppliers. In any case there is no guarantee that the firmware engineers use radios outside of the lab.

If the issue is the result of a SOFT LOCKUP, sending a command to the repeater via an attached HRI-200 may resolve the issue. This may only require switching to the repeater page in the WiRES-X software an applying the repeater's settings with the same value.

If it is a HARD LOCKUP, the only solution is to reset the microcontroller. I.e., turn the power off then on again. Ouch!

- The simplest way to address this problem is to take a timer plug, set it to turn off during a time the repeater is not likely to be in use, then turn it on again as quickly as possible. You may have to put up with a continuous carrier for a good part of 24 hours, but at least you won't have to drive to the hill.
- If there is Internet connectivity at the repeater site, you might be able to use a Wi-Fi enabled power switch to cycle power remotely. (I do this using my home automation.) Unfortunately this requires the action of a control operator.
- Since it is unlikely Yaesu will fix this problem, the ultimate solution is to have a circuit that will automatically reset a lockup condition. Thus we have the De-lockup Project (below).

De-lockup Project

Attached to this post is a project that will automatically reset a locked-up repeater. The concept was originated by Mike, W0IH. Mike informs me that he does not have the bandwidth to provide support for this project in the long term. It is likely we will be refining the project as time goes on. One thing I'd like to do is eliminate the need for a cheap SWR meter. You can obtain a zip file of the project from here.

The project uses an inexpensive Arduino Uno microcontroller board. In addition there is a relay board plus a few extra components. The circuit does not require you to even take the cover off of your repeater and therefore will maintain the warrantee. You can learn more about Arduino at The Arduino home page.