What’s The Worst That Could Happen? RF Communication Disasters

The morning of December 4, 2011 began normally for the team of Air Force technicians. As they settled into their shift flying unmanned aircraft over Afghanistan, perhaps they chatted casually and swapped stories from the weekend. Very soon, however, their conversations were interrupted by shrill alarm sirens blaring from their control monitors. The video screen on the wall, which normally displayed real-time video imagery from their stealth RQ-170 drone, was now completely black. Somewhere near the border with Iran, their multi-million dollar jet was flying blind - no longer responding to any commands or returning any information. Two minutes. Five minutes. Ten minutes of frantic troubleshooting procedures, and the screens were still black. The operators tore through emergency procedure manuals, desperately searching for a sequence of commands that might restore communication. After several frustrating hours without a response, the team knew that their aircraft would not be returning to base.

The details of the chaotic scene described above are based on speculation, but the aftermath is well-documented. Several days later, the Iranian government released photographs of its military officials posing with what appeared to be a largely intact RQ-170 drone. More shocking still, Iranian officials claimed that they actively hijacked the drone using advanced electronic warfare techniques, jamming the communication signal and forcing the aircraft to land safely within their borders. These claims are impossible to verify, but if true they indicate that an RF communication system vulnerability gave Iran possession of one of the most sophisticated devices in the US intelligence arsenal.

Figure 1. The RQ-170 Sentinel drone purportedly downed by Iran in December
Photo courtesy ABC News

For those of us working in the RF communication test industry, stories like this keep us awake at night. Our minds race with questions: How were these communication links tested? Could this have been prevented with more thorough testing? How can we keep this from happening again? Regardless of how a state-of-the-art American UAV ended up in Iranian hands, this situation highlights the vital need for engineers to design and test RF communication equipment under the absolute worst case mission conditions.

Don’t we already do this?

To an engineer, testing for worst case conditions sounds obvious. Any complex system is designed to meet a long list of operational requirements, each with a range of acceptable values. Engineers typically test behavior at the high and low ends of these ranges to cover the “worst” cases. The problem arises when the written requirements or the equipment used to test them do not reflect the full complexities of live mission environments. Stories like this teach us that we need to think far outside of the box when defining and testing the worst case communication conditions.

The basic RF communication issue in the case of the purported UAV attack is interference: an unauthorized signal transmitted within a frequency range allocated for an authorized purpose. What does it mean to test for “worst case” interference? Sometimes interfering signals have low power levels, and they degrade the quality of the data received on the other end of the link. However, high power interference can cause total loss of data at the receive site. Reportedly, the American UAV was blinded by a high power interfering signal in its control channel. Clearly, it is necessary to test modems, radios, and other communication equipment under interference of all severities, including the case when the link is rendered entirely inoperative. Only then can engineers qualify the system behavior under the true worst case scenario.

Other ingredients of disaster

Interference is a huge concern in today’s crowded frequency spectrum, but it is only one of many RF effects that are sometimes overlooked during RF communication testing. Dynamic Doppler effects, atmospheric and multipath fading, noise, and time delay all play significant roles in system performance, and their worst case effects are easy to underestimate. Figure 2 lists a few standard RF effects and scenarios that wreak havoc on communication links.

RF Signal Effect	Worst Case Scenario
Doppler shift	Maximum relative velocity between transmitter and receiver
Fading	Maximum distance, heaviest atmospheric effects, severe dynamic multipath losses
Noise	Antenna pointed toward noise source, like the Sun
Time Delay	Maximum distance between transmitter and receiver
Interference	High power signal causing 100% data loss

Figure 2. Worst case RF communication examples

For example, consider the Cassini-Huygens probe that landed on Saturn's moon Titan in 2005. Only after the spacecraft was halfway across the solar system did engineers discover they had launched the probe with a potentially-fatal flaw in the communication system. They realized that when the landing module separated from the orbiter for descent to the surface, the relative velocities between the two modules would distort the communication signal significantly due to the Doppler effect. The design accounted for the Doppler frequency shift, but because higher frequencies are shifted more than are lower frequencies, communication signals also suffer a throughput loss as the available "data pipe" is effectively constricted. With the planned Cassini-Huygens flight path, the data bit rate changed more rapidly than the receivers could tolerate, and it would cause a loss of communication. To work around the issue, operators actually altered the trajectory of the spacecraft, creating lower relative velocities with less severe Doppler effects. The traditional Doppler test methods used by the engineering team did not model the worst case dynamic Doppler compression. Worst case Doppler effects, which shifts the frequency and constantly changes the bit rate, must be tested at the maximum relative velocities encountered during a mission.

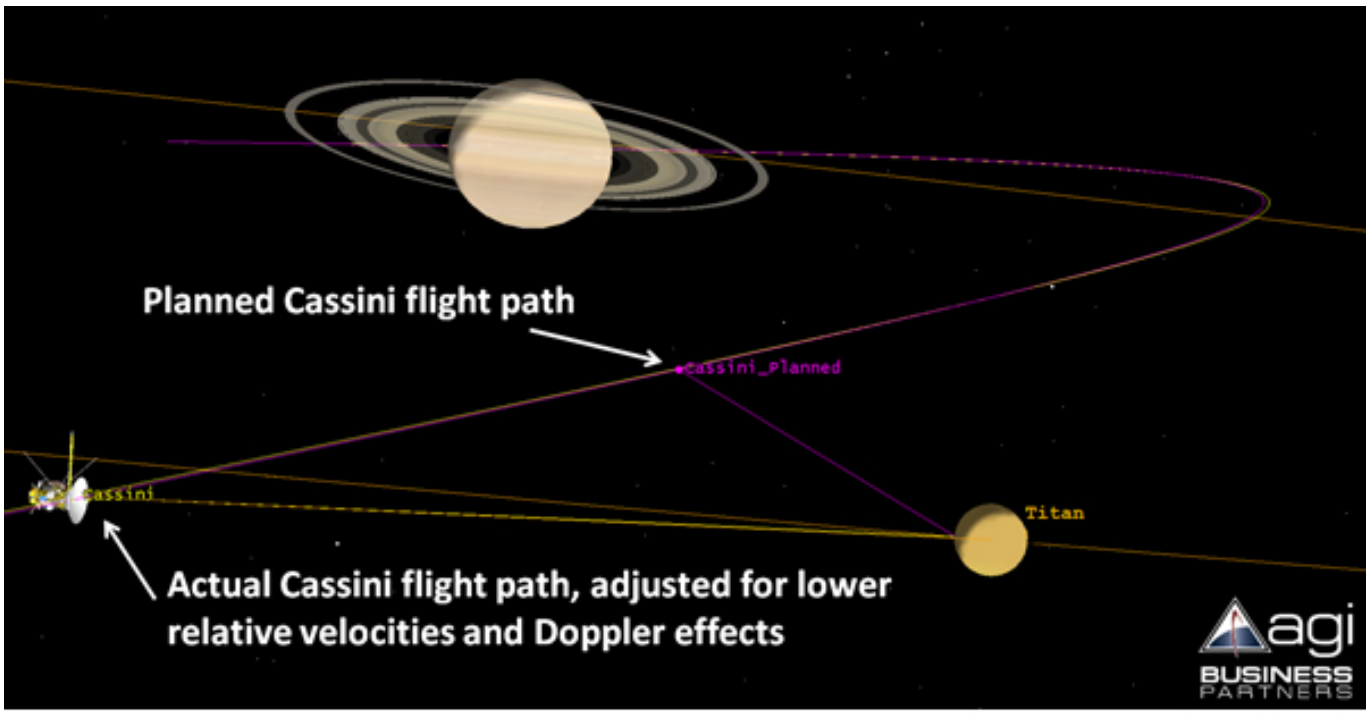

Figure 3. Cassini-Huygens flight path alteration, required to prevent communication system malfunction

Wanted: disciplined test engineers

Testing worst case RF conditions is possible today, but it does require a diligent approach by engineering teams. They must conduct detailed studies of actual mission conditions, employ sophisticated hardware-in-the-loop bench simulation, and perform live-fire testing. This approach is time-consuming, expensive, and tedious, but these investments pale in comparison to the cost of mission failure. Fortunately for engineers, continued innovation in the test and measurement industry is reducing the cost and complexity of disciplined testing. Real-time RF channel simulation instruments can impart worst case physics effects into waveforms, quickly creating an accurate representation of live communication signals. By inserting channel simulators between modems, radios, transmitters, and receivers, test engineers are able to qualify performance of the equipment for the most punishing RF environments encountered in nature. Testing worst case conditions requires extra rigor from engineers, but it ensures their mission will not be remembered as one of our nation's great communication disasters.

About the author

Michael Clonts is a Product Manager in the Signal Instrumentation group at RT Logic. He has more than 10 years of software and firmware development experience in the SATCOM and data storage industries. He received a B.S. in Computer Engineering from Texas A&M University. RT Logic, 12515 Academy Ridge View, Colorado Springs, CO 80921, 719-598-2801, mclonts@rtlogic.com [1]

Additional resources

Dynamic RF Modem Testing Tutorial:

http://www.comsoc.org/form/tutorial-registration-dynamic-rf-modem-testing [2]

October 2012

Source URL (retrieved on *03/10/2014 - 3:52pm*):
http://www.wirelessdesignmag.com/blogs/2012/10/what%E2%80%99s-worst-could-happen-rf-communication-disasters?qt-blogs=0&qt-digital_editions=0

Links:
[1] mailto:mclonts@rtlogic.com
[2] http://www.comsoc.org/form/tutorial-registration-dynamic-rf-modem-testing