Institute of Navigation

International Technical Meeting, Reston, VA

29 January 2019

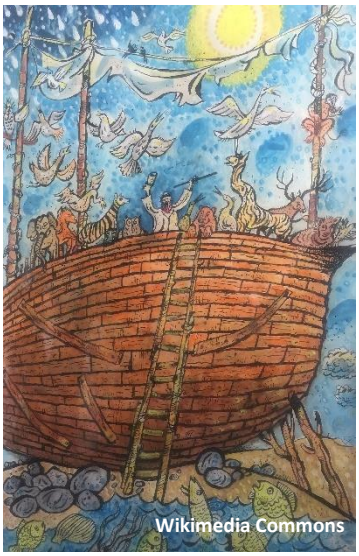
Keynote Address

Mr. Dana A. Goward

GNSS – From a Single Point of Failure to Multiple Points of Success

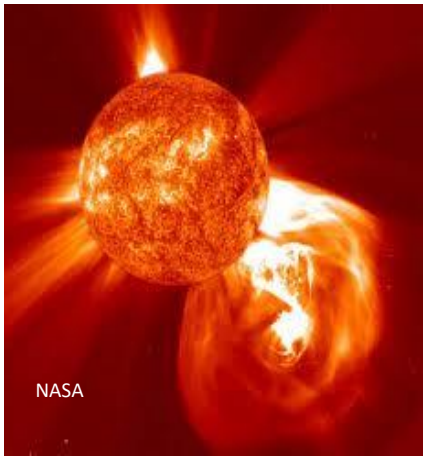
or

How to Avoid a PNT Zombie Apocalypse



This morning's reading is from Genesis, Chapter 9, beginning at Verse 8 –

Then God spoke to Noah and to his sons with him, saying: "…behold, I establish My covenant with you and with your descendants after you… Never again shall all flesh be cut off by the waters of the flood; never again shall there be a flood to destroy the earth… This is the sign of the covenant which I make between Me and you, I set My rainbow in the cloud, and it shall be for the sign of the covenant between Me and the earth." – So sayeth the Lord.



Unfortunately, God didn't say anything about not sending massive solar flares to destroy our satellites and fry ground electronics sending civilization back 200 years.

My message to you today is that GNSS and PNT are vital to the wellbeing of our nations and the world, at the moment they are fragile, and we all have a responsibility to do everything we can to protect them.

At this point many of you, especially if you have heard me speak before, might be saying "there he goes again with the PNT zombie apocalypse scenario. What is with this guy?"

A couple points in my defense.

First, it's important for good systems engineers and policy makers to worry about rare but high impact and catastrophic scenarios. All too often people unconsciously equate "rare" with "it will never happen" and then are punished by the phenomena of large numbers.

> *In 1986 the Riverwalk shopping mall was built on wharfs lining the Mississippi in New Orleans. Huge ships passed by that spot everyday. The builders thought that it was one in a million chance this would be a problem, so did nothing to protect against it. The mall had been in operation for ten years and an estimated 600,000 ships had safely passed by when a 700 ft vessel sailing down the river lost power. The 36,000 ton bulk carrier slammed into and destroyed most of the mall. One in a million wasn't protection against a problem, it was assurance there would be one.*

The second thing I'd like to say my defense is that we have some records of near-zombie apocalypse occurrences in the GNSS world.

Cybersecurity of the constellations themselves has not been a problem …yet… as far as we know. But we have seen some pretty interesting failures and glitches with GLONASS and GPS. These are very complex systems. And the more complex the system, the more likely internal failures, unintended effects, and the more consequential the impacts of human error.

Then there is the sun. Considering how recently we began serious study of solar activity, we have a very interesting record.

Everyone knows about the Carrington Event of 1859 that set telegraph offices on fire and brought the northern lights to Tahiti.

Less well known is the 1921 NY Railroad storm, so called because it set a control tower for the NY Central Railroad on fire and stopped service below 125th street. Telegraph service across the US was slowed and then stopped, aurora were observed in Puerto Rico, and other effects were felt around the world. This storm was estimated to be about ten times stronger than the one that blacked out Quebec and other parts of the northeastern part of the continent in 1989.

In 2012 a coronal mass ejection intersected Earth's orbit at a spot our planet had been in just a week before. It was estimated to have been at least as strong as the Carrington event. According to NASA scientists, if it had hit, we would still be picking up the pieces. They estimate that the chances of a similar event making contact in the next 10 years at 12%. In the next 50 years, about 47%.

To quote Clint Eastwood in the film *Dirty Harry* "…you've got to ask yourself one question: 'Do I feel lucky?' Well, do you…?"

And the sun is only one of a number of threat vectors that could cause disastrous consequences. So catastrophic scenarios are something we should take seriously. And something we should act now to prevent. Because we might not have 50 years. We might not have 50 days.

But its very hard for people, especially policy makers, to take action to prevent bad things from happening. Reacting after the damage has been done is psychologically much easier for some reason.

> *There's a great story in the book "The Black Swan" about Farmer Brown's turkey. The turkey has the best life available. A warm, safe shelter and every day at 8:00 in the morning Farmer Brown comes by to feed him. This has been going on for 300 days in a row and there is no reason for the turkey to think this isn't going to go on forever. But of course, tomorrow is Thanksgiving.*

Even the smartest people have a tendency to take what has happened in the past and extrapolate it in a straight line when they think about the future.

Also, most of us tend to think of rare, high impact events as random and unpredictable. Lots of people look at airplane crashes that way, for example. I have a background in aviation safety and I can tell you that every aviation accident investigation I know of has shown precursor events and indicators which, if someone had been paying attention, could have been used to avoid the disaster.

The same is true in the GNSS/PNT world. Signals and systems are disrupted everyday. Europe's STRIKE3 project found over 250 families of jammers operating on the continent and hundreds of thousands of accidental and intentional disruption incidents.

These tens of thousands of daily PNT disruptions can be a great help to us, if we let them. They highlight the extreme vulnerability of an essential service, and they can serve as warnings of larger problems to come.

The question is, are we willing to do anything about stemming the tide of small problems and preventing the big one?

We at the RNT Foundation, as you probably know, advocate a holistic approach to transforming GNSS signals from a single point of failure for most first world societies into part of a robust PNT architecture that has multiple points of success. We support a systems engineering approach to this problem and summarize it as Protect, Toughen and Augment.

> *A delivery driver uses a small jammer to hide his movements from his employer. Jammers and spoofers are used to highjack valuable cargo. Aircraft circle the airport another time when stray signals disrupt GPS. Yet the technology and equipment to detect and locate these transmissions are inexpensive and readily available.*

We all need to protect GNSS frequencies and signals from disruption.

> *At the PNT Advisory Board several years ago we had an industry group give a presentation. They told us of a shocking discovery. That when they purchased their GNSS receivers at Walmart and had Joe the plumber install them in their network, things didn't always work out so well.*

Software and hardware that can make receivers much more reliable and resistant to interference are available. They just need to be used.

Toughened receivers are common sense and essential. The fact that so few are in use now shows ignorance and indifference by users, and a failure of manufacturers and others in our community to educate them.

And don't whine to me about how much more good equipment costs. The next time someone complains to you about cost, ask them if they are still using a flip phone. Or if they have a tube TV set at home.

We also strongly support augmenting GNSS with other PNT sources, including a terrestrial, wireless precise navigation and timing signal.

Numerous studies have shown that combining space-based PNT with a terrestrial wireless PNT system that has greatly different phenomenology could make users virtually bullet proof to a whole range of threats from delivery drivers to massive solar flares.

Some nations like China, Russia, Saudi Arabia and South Korea already have terrestrial wireless PNT systems that could be used if space systems were not available. It is hard to say how much they have integrated them into critical infrastructure and applications. But the systems have been on-line for

decades, with known signal structures and available receivers. If they are not taking full advantage of them for national and economic security, mores the pity.

Other nations have started down that path.

The United Kingdom, as an example, is concerned about Coronal mass ejections and a PNT zombie apocalypse. It has been on their national risk register for several years. This resulted in a 2017 London Economics report showing that the UK economy would lose $1.3B/day during a GNSS outage, and a 2018 government report that called for a number of actions to guard against such an eventuality.

Unfortunately, since then their nation has been roiled by political divisions and controversy. Progress on most things has come to almost a complete halt. - Good thing we don't have those kinds of problems on this side of the Atlantic.

Of course, we do have our own challenges here in the US. While administrations have talked a good game about augmenting GPS since 2004 when President Bush directed we get a backup capability, they haven't really done much.

Fortunately, Congress has increasingly been concerned and interested. In 2018 $15M was appropriated for a GPS backup technology demonstration, and the National Timing Resilience and Security Act was signed into law. This act requires the Secretary of Transportation to establish a wireless terrestrial timing system as a backup for GPS timing by 2020.

At this point you are undoubtedly saying to yourself "Golly, this is important stuff. But what can I do to help?"

Good question, thanks for asking!

One thing that immediately comes to my mind is that you could join, or get your company to join, our charity the RNT Foundation, which advocates for policies and systems to protect GNSS signals and users.

You could help the standards group SAE develop standards and recommendations for resilient GNSS receivers. Let me know afterward if you would like more information.

Perhaps most importantly, though, is that you can leverage your own expertise and voice to make a difference locally and nationally.

But PNT experts have been speaking up for years, you say. Why aren't we further along than we are? Again, good question;

The answers are many, varied and I could drone on all day about them.

But in my mind, they all boil down to the immortal words of the actor Strother Martin playing a prison Boss in the movie "Cool Hand Luke." Just after he had beaten a prisoner, played by Paul Newman, for some small infraction, Strother assessed the situation by saying "What we got here, is failure to communicate."

> *Many years ago, two pilots for the Texas Air National Guard were out on a training flight in their C-130 aircraft. After making several practice landings they lined the aircraft up with the runway for another "touch and go." As they approached the field, the lead pilot noticed that the aircraft was descending too fast. Wanting the throttles advanced full forward so they could climb out, he called for "Takeoff Power!" The co-pilot took off power and they crashed short of the runway*.

"What we got here, is failure to communicate." Two professionals, trained in the same discipline, disastrous results. How much more difficult is it then, for people from completely different backgrounds to understand each other? Engineers and politicians, for example. Two groups who couldn't be farther apart in many ways.

> *Several years ago, a US a high-ranking government engineer and technologist was concerned that our politicians did not appreciate the importance of GPS and the need for a complementary backup system in the event GPS was disrupted. To make his point he commissioned a study to quantify GPS' economic benefits. The study found that the direct economic impact was approximately $96B/yr, GPS timing was essential for 13 of 18 critical infrastructure sectors, and that there were large, but difficult to quantify, secondary and tertiary impacts to all aspects of the economy and society. His conclusion was that a complementary backup position, navigation and timing system, with different failure modes than space-borne systems, was an essential component of a rational national and homeland security architecture, and should be expedited.*

Nothing much happened.

Compare that approach to the ways politicians talk to each other with emotionally impactful stories:

> *"When GPS fails, every mode of transportation will slow down and become more dangerous. Many drivers won't be able to find their way and will be even more distracted than normal. There will be more accidents and probably more fatalities. First responders' radio and dispatch systems will work poorly, if at all, and responses will be further delayed by navigation and traffic problems. Then, as backup clocks in various networks desynchronize, cell phone networks, ATM and credit card transactions, everything that depends upon a network, will begin to fail. And these days, pretty much everything depends upon a network.*

This kind of scenario-based story telling has engaged elected officials, spawned half a dozen Congressional hearings, and contributed to seven pieces of legislation that have been signed into law.

So, point number one - The language in which a message is delivered is as important as its content. Speaking Russian will get you nowhere if the person you are trying to reach only understands Urdu.

Stories of white van man disrupting an airport landing system go much farther than an analysis of unlawful spectrum interference.

> *You have probably heard the old story from back in the days of the draft about the sad sack soldier who, wherever he went, would pick up pieces of paper, look at both sides and say "No, that's not it." In the barbershop, in the mess hall, everywhere he went he would pick them up and say "No, that's not it." After months of this, word made its way to the post psychiatrist. The doctor was appalled by this behavior and the soldier was promptly designated unfit for duty. Of course, when he was handed his discharge, the solider looked at the paper and said "Yes, this is it!"*

There are a couple lessons about communication in this tired old joke.

First, brevity, clarity, consistency and emotional impact are key. This guy didn't think he belonged in the Army, and he had a very effective way of showing it. Also, he communicated his message to everyone he met – very important, when trying to influence a large organization, especially if it is a popularly elected government. You never know when you might be dealing with someone who is a key influencer, or even the person who can give you what you want.

And he was persistent. This is especially important in democratic public life. The signal to noise ratio is very, very low, and on top of that, few people are searching for your signals. So you can't give up until you get through.

My final point for you today is the old adage that "To whom much is given, from them much is required."

Too often, people with special knowledge and understanding, for one reason or another, fail to make themselves heard.

> *Before Hurricane Katrina I served at the Coast Guard Air Station in New Orleans. Every year folks from the Army Corps of Engineers would come to our training day and tell us "When the levees fail, you need to have a hand ax in your attic so you can chop your way out… Not "if" the levees fail – when the levees fail. They understood the system, had observed minor failures, and knew that a major event was just a matter of time.*
>
> *Before 9/11 over 130 passenger aircraft had been hijacked. Aviation security experts in this country had long called for simple security measures like reinforcing cockpit doors on airliners, as the Israelis had done. These experts understood the system, had observed minor failures, and knew that a major event was just a matter of time.*

The list of examples of experts unable to make themselves heard and ensuing tragedy is nearly endless.

Yet, while it is less well known, the list of experts preventing bad things from happening is even longer. The fact that humanity hasn't yet been wiped out by nuclear war, Ebola, or suffered a multitude of other potential disasters is proof positive.

Everyone in this room is blessed to be a well educated and well regarded citizen of a free society. And our elected leaders are compelled to take notice of us, despite how it may appear sometimes. That makes us powerful and important people.

All of us in this room have important special knowledge about our nations' PNT security that we have a duty to share. We understand the system, have observed minor failures, and know that a major event is just a matter of time.

We know that, until there are multiple, resilient independent sources of PNT, and they have been incorporated into our critical infrastructure, our nations will be at unacceptable risk. We are painfully aware that space is not enough

– we also need down-to-earth solutions. We need a healthy, balanced and resilient PNT system. We need to protect, toughen, and augment.

When you leave this place, please take with you a commitment to share your knowledge in a way that is understandable, brief and consistent, and with as many people as you are able. Your personal networks extend far further than you know, including into the highest reaches of government and society. Use them. Act locally, think globally and do all you can.

And if we are lucky, we might even avoid a PNT zombie apocalypse.