Jamming and Spoofing of GNSS Signals – An Underestimated Risk?!

Alexander Ruegamer and Dirk Kowalewski (Germany)

Key words: GNSS/GPS; Professional practice; Risk management; Jamming; Spoofing

SUMMARY

GNSS technology is used for many applications: The surveying industry uses GNSS for monitoring the continental drift, stakeout fixed-points, measuring maps of areas and many other location based services. The construction industry uses GNSS for machine control and logistics, the agriculture for precise farming, power steering assists and other tasks like manure, reaping and plowing. Since the last 10 years GNSS also entered in many daily life applications like car navigation and location based services (Google Maps, Facebook). But GNSS is also used as a sensor for many safety-critical applications: the example of guided landing approach of airplanes is well known but it is less known that GNSS – and here specific the Open Service of the US NAVSTAR GPS – is used as a crucial sensor for timing and synchronization of reference stations for telecommunication, electrical power supplies, exchange markets and banks. For many years the availability and faultless function of GNSS was taken for granted. Jamming (the intentional interference targeting the unavailability of the system) as well as spoofing (the faking of a false position/time towards a target GNSS receiver) was no concern for nearly all users except the military. But recent events started a gradual paradigm shift: the unintentional jamming of the Newark Airport, NY, USA by an UPS driver with a US$ 100 devices available on ebay; the capturing of a US drone using a GPS spoofer by Iran; the demonstration of students from the University of Austin, Texas, US to hijack a US$ 80 million dollar Yacht with a self-made spoofer as well as their laboratory demonstration to use this spoofer to tamper the phase measurement units used for energy network synchronization and control. In this paper we review these events and show how our currently used GNSS technology was attacked and affected. Then we discuss different measures to detect and even mitigate these threats on algorithmic, receiver, antenna and system level. Finally, we conclude with providing solutions and recommendations for hardening and protecting GNSS receivers by e.g. using array antennas and/or services like the Galileo Public Regulated Service (PRS) with civilian anti-spoofing guaranteed by the strong encryption used there.