A Risk Analysis of Communication, Navigation and Sensing Satellite Systems Threats

Homayoun Nikookar

Faculty of Military Sciences, Netherlands Defence Academy – Den Helder
E-mail: h.nikookar.nl@ieee.org

Received 30 April 2022; Accepted 31 May 2022;
Publication 20 September 2022

Abstract

The use of space systems to support Communication Navigation Sensing and Services (CONASENSE) activities has increased exponentially since their first application in 1965 with the Initial Defense Satellite Communications System. Although the first major application was for communications services, space-based capabilities have now expanded to provide a wide range of other types of services. Today these applications include navigation, targeting, mapping, remote sensing, surveillance and meteorological tracking, prediction and other services [1, 2]. Currently space is seen as a new frontier in which satellites play a major role. Given the importance of CONASENSE satellite services in today's life and huge amounts of financial resources and the state-of-the-art technological capabilities, that are necessary to realize this kind of technology, it makes a satellite system a realistic target for threats. Currently cyber threats are becoming the most obvious resources to take adversary action against CONASENSE satellites. In addition to that the ground control stations and antennas will also be vulnerable to cyber threats and conventional threats as well. In this paper the threats of CONASENSE satellites are studied and a risk analysis of the relevant threats is provided. The

Journal of Mobile Multimedia, Vol. 19_1, 277–290.
doi: 10.13052/jmm1550-4646.19114

influence of artificial intelligence (AI) technology and the role it can possibly play in protective measures are also included.

Keywords: Communication Navigation Sensing and Services (CONASENSE) Satellites, threats, risk analysis, protection measures.

1 Introduction

The threats to CONASENSE satellite systems are split into two categories: (1) Atmospheric threats; like solar flares, space debris, thunder and volcanic activities and (2) man-made threats; like kinetic energy threats (KET), nuclear, laser and cyber threats. Each paragraph below will elaborate on the likelihood of occurrence, the damage tit can cause, which components of the satellite system are affected and most importantly how the threat can be averted or countered. Following each category a summary of all identified threats, their occurrence and impact on the system are provided.

2 Atmospheric Threats and Countermeasures

The most occurring threats for CONASENSE satellite systems are atmospheric threats. These include not only earth atmospheric threats like clouds, rain and thunderstorms but also solar flames and other naturally occurring space threats like asteroids and meteorites.

2.1 Earth's Atmospheric Threats

First of all, the earth's atmospheric threats are discussed as these are the most occurring threats. Atmospheric conditions, like clouds and rain, can form a significant threat to the radio channel of CONASENSE satellite systems. This effect is comparable to the WiFi signal strength inside home. When we have a clear path to the router, high frequency radio transmission is favorable. However, when the path is obstructed by objects in the environment such as walls, a lower frequency band is favorable as the lower frequency signals pass more easily through/around objects. On the other hand, thunderstorms form a threat to a much wider range of satellite systems due to the charged particles and currents present in the thunderclouds. These particles have a strong impact on the channel between the satellite and ground station in such a way that the connection can be temporarily disrupted or paralyzed, independent of the used frequency band. Although thunderstorms can form a

threat, the likelihood of occurrence is low compared to 'normal' atmospheric conditions as clouds or rain.

Furthermore, there are extreme situations that form a more serious threat to CONASENSE satellite systems like volcanic activities. Lava forms a great threat to the Ground Control Station (GCS) and its components, like antennas or the local power grid. However, the main threat of a volcanic eruption is not the lava but the ash clouds it generates. These clouds can reach up to 45 kilometers height [3] and disrupt the channel between the satellite and ground station due to the physical blockage of the signal by (sometimes charged) particles. However, volcanic activities of that scale are rare which makes the total involved risk small. Besides a low occurrence, this threat can be countered by not building the GCS in the close proximity of an active volcano.

2.2 Space Weather

The second kind of atmospheric threats occur outside of the earth's atmosphere and can be summarized as space weather. The term space weather generally refers to conditions on the sun, in the solar wind, and within Earth's magnetosphere, ionosphere and thermosphere that can influence the performance and reliability of space-borne and ground-based systems and can endanger human life or health as well [2]. Although solar flares are rare, the threat they form against CONASENSE satellites is severe. Solar flares emit charged particles and high energy waves which can damage the electrical systems onboard the satellites. Solar flares do not pose a threat to the GCS and channel because the earth's magnetic field acts like a shield against the particles. In most cases, the effects of a solar flare are not that devastating and only impact the performance of the satellite. However, the protection against solar flares must be taken seriously and may include special shielding materials that form an extra protecting layer for critical systems.

Another threat which exists beyond the earth's atmosphere is space debris. Space debris exists in multiple forms varying from naturally existing debris like meteorites and asteroids to man-made debris like decommissioned satellites. Almost all debris will burn up in the earth's atmosphere and will pose no threat to the GCS. On the other hand, all types of debris do pose a threat to the CONASENSE satellites in orbit. Even smaller sized meteorites, which often travel in meteorite clouds, could collide with the satellite and instantly destroy it. Besides this, the most dangerous effect of a meteorite cloud is that it can damage multiple satellites in a short time

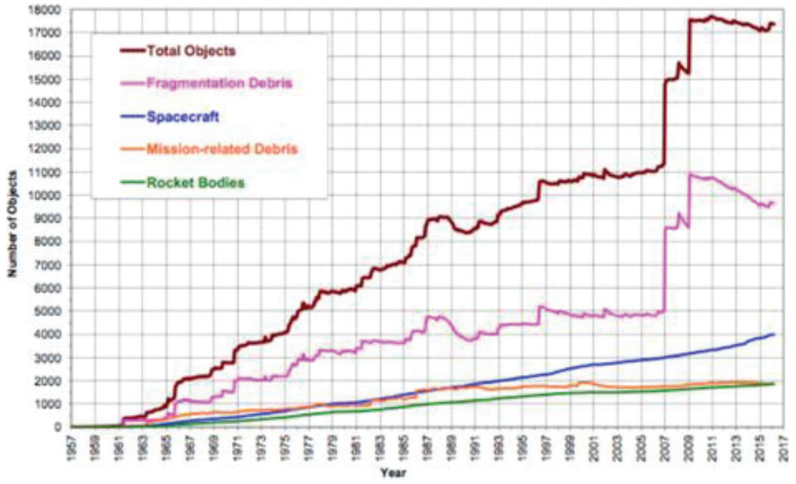


Figure 1 Objects in earth's orbit over the years [5].

span. The satellites that get hit, may break into more pieces and thus create more debris. With the increasing number of satellites in the earth's orbit [4], this becomes a more and more severe threat. Figure 1 shows the objects in the earth's orbit over time. It is not possible to protect a satellite against the impact of space debris, however, it is possible to spread the satellites in their orbit to prevent clustering. By doing so, the snowball effect will be minimized when a satellite collides with space debris.

Since the beginning of space exploration up until the year 2009, there were no rules for decommissioned satellites since space was a new and pioneering domain that had no international overarching governance. Since then, the satellites that are no longer functional need to be sent either further in space or back to earth to burn up in the atmosphere to stop the saturation of orbital objects. The decrease of orbital objects since 2009 can be seen in Figure 1, [5].

3 Hostile Threats and Countermeasures

The threats that form a high risk to the satellite system are rare when these threats come from natural atmosphere. With increased capabilities and growing dependence on civil and military uses of satellites, satellites of all sorts have automatically become a target for hostile intent. The threat to satellites is posed by various types of anti-satellite approaches. Classic kinetic

threats, state of the art laser - and cyber weapons form a threat to the satellite systems. All of these threats can be summarized as space threats. A space threat is that which can damage, destroy, permanently disrupt the functioning of, or change the flight trajectory of space objects of other states. These space threats are generally divided into three classes: (1) Nuclear, (2) non-nuclear and (3) cyber threats, which are threats that do not damage the physical satellite but destroy the Command Control (C2) or surveillance equipment to disable the satellites' operations. The threats have a wide range of deployment methods: ground- space, space-space, space-air, space-ground and air-space. Since the space domain is relatively new, most of the threats are conceptual or currently being developed which makes it hard to estimate the operational capabilities of a threat.

3.1 Nuclear Threats

Let us start with the first class, nuclear threats. Obviously, this forms a threat to a satellite system. The GCS and its systems can be destroyed by the blast of the explosion. The electromagnetic pulse (EMP) that is produced by the nuclear fission has the same effect as charged particles of a solar flare and can fry electrical circuits of the GCS systems leaving them permanently damaged. Depending on the altitude and the payload of the explosion, the resulting EMP can have a very great range. The threat is than effective against the channel part of the satellite system, cluttering it with charged particles and high energy waves leaving the channel blocked for any communication. When a nuclear weapon is carried up to space and is detonated in orbit, the effects on the GCS systems or the channel would be minimal. However, the effects on the satellites in the vicinity of the explosion could be devastating. Satellites near the explosion would instantly vaporize by the heat of the explosion. Since there is no medium in space, there is no shockwave that damages the satellites. The EMP produced by the nuclear fission will do the most harm to the on-board systems by frying their electrical circuits.

3.2 Kinetic Energy Threats

The second class of space threats is also the most extensive threat. These threats are categorized as the non-nuclear threats and are also known as Kinetic Energy Threats (KET) and range from classic kinetic weapons such as ballistic missiles to state-of-the-art leaser technology weapons. The intention of KET's is to physically hit a satellite that is in low orbit, or on its way to orbit, with a co-orbital-/ground-/air-based system to destroy it. Although

this is an effective way to destroy a satellite, it is still a major challenge to hit a satellite in orbit with conventional weaponry which requires very precise tracking capabilities that is only available to highly developed organizations. While these threats have the ability to destroy low earth orbital satellites (LEO), they still have a few major downsides. Anti-satellite KET take a long time to reach their target which may give enough time to react to it. Launching KET is also heavily dependent on technological and financial resources and not to forget is a great risk of launching failure. The greatest downside to this kind of anti-satellite threats is that an impact in space can result in a lot of space debris from the satellite that can harm other satellites that were not intended as a target. This space debris can set of a chain reaction as discussed in the previous section. Although the chance of such a KET hitting a satellite is small, it still forms a big threat to satellite systems.

The KETs do not only form a threat towards the physical satellite, but also to the GCS component of the system. It is very easy to destroy a GCS or its systems with today's arsenal. In fact, effects of destroying a GCS can result in a similar effect for a satellite system as destroying the physical satellite, but with way less resources to spend. Although a GCS system is replaced or rebuilt more easily and faster, often human casualties are involved by its destruction with KETs which makes the threat possibly larger compared to the threat of losing a satellite depending on the ethics standpoint of the operating actor.

3.3 Cyber Threats

Lastly, the most common man-made threat against a satellite system, the cyber threats will be investigated. These threats are the easiest, most affordable and most accessible threats to any satellite system. The most important thing about cyber threats is that it forms a threat to all elements of the satellite system. It can even threaten the elements all at the same time. But let us start with the threat to the GCS's systems. The computer- and antenna systems that are used to monitor, communicate, maintain, steer and update the satellite are vulnerable to all sort of cyber threats such as viruses, ransomware or other forms of malicious software that have the intend to have a harmful effect on the satellite's operations. Since the GCS's systems are the primary channel to communicate with the satellites, these have to be secured the best since they control everything onboard the satellite. Simply jamming antennas of a GCS is a cheap and easily accessible way that does not require any advanced scheme to disrupting a satellite system. It is therefore a must that vital systems on the ground are build redundant to overcome such easy threats.

The systems onboard the satellite are also vulnerable to cyber threats. Therefore, the onboard systems also need to be protected just like the GCS's systems. The best option would be that the satellite is like a closed box that performs its tasks but can only be influenced via a channel coming from the GCS. When this single channel is secured (encrypted) correctly, the cyber risks of the systems onboard the satellite are minimalized.

3.4 Artificial Intelligence (AI) as a Counter Measure

Some countermeasures to a specific threat have already been discussed in the previous sections. This paragraph focusses on the possibilities to use artificial intelligence (AI) to increase the reliability of satellite communication. AI can generally be used in two ways to increase reliability. First, AI can be used in a preventive manner. The prediction of space weather is a good example where AI can play a valuable role. This is currently done by collecting data from Earth's orbital sensors like telescopes and satellites. The conversion of this data to usable information is difficult due to the large size of the data and the complex calculation and prediction matrices. The computational power of AI can be put to great use in these applications. When a more precise prediction of space weather can be made, the consequences of space weather can be minimized as proper preventive countermeasures can be taken on time. Also, the reaction time to act on the current situation of space weather is greatly increased. Nowadays, orbital sensors detect these 13 minutes before the first effects of the solar flare are present around Earth. The secondary effects arrive after 30 to 72 hours, which is still a short time to undergo protective measures [6]. When an accurate prediction of space weather can be made a week ahead or more, engineers can take better preventive actions to counter the effects of space weather. Also, the manual labor that is saved by the utilization of AI techniques can be used efficiently elsewhere.

Secondly, AI can be used as a protective manner specifically against cyber threats. Nowadays GCS's are heavily dependent on cyber physical systems. These GCS's systems are used for the communication, maintenance and steering of the satellite and can be seen as mission critical systems. It is therefore vital for the perseverance of the satellite system that these ground systems are not vulnerable to cyber threats. Since these systems become more complex and integrated every day, maintaining cyber security is becoming a real challenge. This means that keeping cyber physical systems secure has almost become an impossible task for human. AI can be used in this scenario as a protective tool for these critical systems. Moreover, as systems

become more complex, the integration between the systems gets harder with each upgrade. Information Communication Technology (ICT) techniques are needed to keep all these different systems compatible with each other. AI can be used as a central managing and integration tool for all systems, which allows different complex systems to integrate. This results in more efficient systems environment where human resources can be used more efficiently.

4 Risk Analysis

In the previous parts of this paper, the threats and their respective countermeasures were discussed. In this section, all these threats are being converted and summarized into a clear risk matrix. The section is divided into three parts, firstly we discuss the risk table. The second part consists of a risk analysis of the earlier discussed threats on a satellite system without protective measures. The last part explains a risk analysis for the same threats but when protective measures are taken.

4.1 Risk Matrix

The risk analyses that are done in this paper are based on the risk matrix. This is a matrix that values a threat into a risk factor, based on the consequence and the likelihood of the threat. This is done by the following formula:

$$\text{Risk} = (\text{Consequence of threat}) \cdot (\text{Likelihood of threat}) \tag{1}$$

The risk matrix that is used in this paper is illustrated in Figure 2.

The goal of the risk matrix is to gain a simple and quick insight into the risk that is formed by a certain threat. This risk is valued by the matrix based on the earlier stated formula (1). The first outcome can be seen as a naked risk since it is the risk without countermeasures. When the risk has been valued, the next step is to lower the risk. This can either be done by trying to lower the likelihood or the consequence of the threat. These two steps will be done in the upcoming sections for the threats against satellite systems that were discussed in Sections 2 and 3.

4.2 Risk Analysis Without Protective Measures

The first risk analysis will reflect on the threats for a satellite system without any protective or countermeasures. This is to gain an insight into the pure risk that is formed by the threat. With this quantified risk, the focus can then

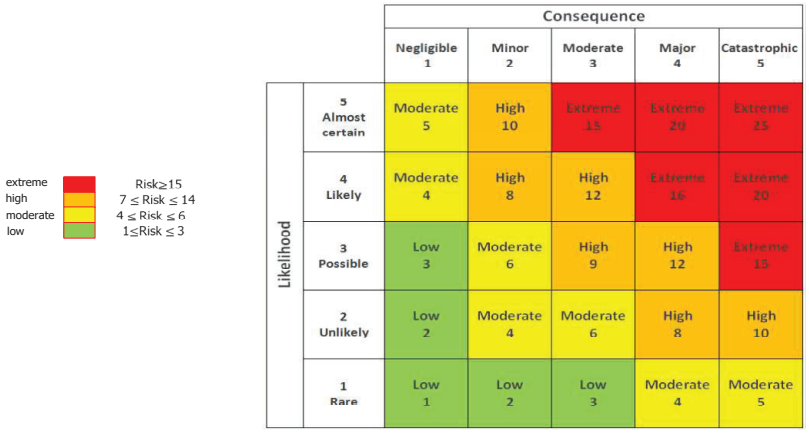


Figure 2 The risk matrix.

be narrowed down on the factor which minimizes the risk if the risk is not accepted in the first place. Figure 3 shows the risk matrix with entries filled based on the results of the first analysis discussed in Sections 2 and 3.

4.3 Risk Analysis with Protective Measures

The second risk analysis will reflect on the same threats for a satellite system as Section 4.2 but now with protective or countermeasures included. The goal is to obviously lower the risk value compared to the first analysis. This can be done by decreasing the likelihood factor or by decreasing the consequence factor. For kinetic energy and nuclear threats, it is very hard to lower the consequence or destructive capability of the threat. Therefore, the likelihood is most of the times decreased to lower the overall risk value. The results of the second analysis are shown in Figure 4.

4.4 Comparison of Risk Analyses

The results of the risk analyses from Section 4.2 and 4.3 are compared to each other to gain insight into the efficiency of the protective measures and countermeasures. Also, the value of the remaining risk after the measures is discussed to sanity check. The results of both analyses are put together in Figure 5.

As Figure 5 clearly shows, all naturally occurring risks are decreased by a factor of 50% while man-made threats are the same or decreased just

Threat	**Satellite system's component**	**Frequency of threat**	**Destructive capability of threat**	**Total risk**
Earth's Atmospheric threats	- GCS - Channel	Almost certain (5)	Minor (2)	High (10)
Space weather threats	- Channel - Satellite	Possible (3)	Major (4)	High (12)
Nuclear threats	- GCS - Channel - Satellite	Rare (1)	Catastrophic (5)	Moderate (5)
KET's threats	- GCS - Channel - Satellite	Rare (1)	Major (4)	Moderate (4)
Cyber threats	- GCS - Channel - Satellite	Likely (4)	Major (4)	Extreme (16)

Figure 3 Risk analysis matrix without protective measures.

slightly. These risk factors are decreased by such a great margin because of the countermeasures against the threats. By a good monitoring and an accurate prediction of natural events, some easy protective measures can be taken. This reduces the impact factor of the threat which will lower the overall risk extensively. The likelihood of a naturally occurring event is hard to counter and is therefore unchanged since it is more effective to monitor and predict the event than to try and counter it.

The man-made threats can however be decreased in both likelihood and impact. The impact factor for kinetic energy threats can for instance be lowered by using good armor or other sorts of protective measures like built-in redundancy. The consequences of a nuclear threat are however unchangeable as their destructive potential is enormous. The likelihood of the usage of such threats stays the same at the lowest, so the risk does not change. After both analyses the cyber threats form the greatest threat. The threat is less

Threat	**Satellite system's component**	**Frequency of threat**	**Destructive capability of threat**	**Total risk**
Earth's Atmospheric threats	- GCS - Channel	Almost certain (5)	Negligible (1)	Moderate (5)
Space weather threats	- Channel - Satellite	Possible (3)	Minor (2)	Moderate (6)
Nuclear threats	- GCS - Channel - Satellite	Rare (1)	Catastrophic (5)	Moderate (5)
KET's threats	- GCS - Channel - Satellite	Rare (1)	Moderate (3)	Low (3)
Cyber threats	- GCS - Channel - Satellite	Possible (3)	Moderate (3)	High (9)

Figure 4 Risk analysis matrix with protective measures.

Threat	**Total risk without protective measures**	**Total risk with protective measures**
Earth's Atmospheric threats	High (10)	Moderate (5)
Space weather threats	High (12)	Moderate (6)
Nuclear threats	Moderate (5)	Moderate (5)
KET's threats	Moderate (4)	Low (3)
Cyber threats	Extreme (16)	High (9)

Figure 5 Comparison of risk matrices.

after some protective measures, especially in the cyber domain. But since this domain is the modern-day threat, the likelihood of the threat even after high-end protective measures (like the implementation of AI techniques) is still possible. Also, the impact of a severe cyber-attack can be moderate even after protective measures for all systems. This is the reality of a digital world that is heavily integrated with and dependent on each other.

The right column of Figure 5 also shows that there are no scenarios where all risks are eliminated after protective measures. This means that in all scenarios a threat can still be imminent no matter how small the impact or the likelihood is. Therefore, caution during the usage of the system is the best protective measure.

5 Conclusion

For the CONASENSE satellite systems different variety of threats and countermeasures were discussed. The threats are divided into two general groups: naturally occurring threats and man-made threats. Naturally occurring threats consist among other of Earth's weather effects and space weather effects like solar flares and meteorite showers. Man-made threats are divided into nuclear threats, kinetic-energy threats and cyber threats. A risk analysis was carried out with the help of a risk matrix to gain an insight into the resulting risk factor for each threat, before and after specific countermeasures. The influence of artificial intelligence and the role it can possibly play in protective and defensive measures was included. The risk analysis shows that cyber threats form the greatest threat to CONASENSE satellites.

Disclaimer

The opinions expressed in this paper are those of the author and do not reflect the Dutch Ministry of Defence point of views.

References

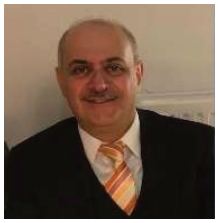
[1] T. C. Tozer, "An Introduction to Military Satellite Communications," Royal Signal Radar and Establishment Memorandum, 1987, https://apps.dtic.mil/sti/pdfs/ADA187005.pdf

[2] J. Pelton, Future of Military Satellite Systems, Handbook of Satellite Applications (pp. 705–719), 2017, DOI: 10.1007/978-3-319-23386-4_107, visited 8 Feb. 2022, https://www.researchgate.net/publication/312455625_Future_of_Military_Satellite_Systems

[3] T. Wilson et al., "Volcanic ash impacts on critical infrastructure," Physics and Chemistry of the Earth, Parts A/B/C. 45–46: 5–23, Elsevier, 2012.

[4] Ry Crist, "Starlink explained," https://www.cnet.com/home/internet/starlink-satellite-internet-explained, visited 9 Feb. 2022.
[5] https://www.researchgate.net/figure/Monthly-number-of-objects-in-the-Earth-orbit-cataloged-by-the-US-Space-Surveillance_fig3_264863542, visited 8 Feb. 2022.
[6] Haidara, F. M. (1995, May). Characterization of tropospheric scintillations on Earth-space paths in the Ku and Ka frequency bands using the results from the Virginia Tech OLYMPUS experiment. Virginia Tech. http://hdl.handle.net/10919/38423

Biography



Homayoun Nikookar received his Ph.D. in Electrical Engineering from Delft University of Technology in 1995. He is an Associate Professor at the Faculty of Military Sciences of the Netherlands Defence Academy. In the past he has led the Radio Advanced Technologies and Systems (RATS) research program, and supervised a team of researchers carrying out cutting-edge research in the field of advanced radio transmission. He has received several paper awards at international conferences and symposiums. Dr Nikookar has published more than 150 papers in the peer reviewed international technical journals and conferences, 15 book chapters and is author of two books: Introduction to Ultra Wideband for Wireless Communications, Springer, 2009 and Wavelet Radio: Adaptive and Reconfigurable Wireless Systems based on Wavelets, Cambridge University Press, 2013.